ベルヌーイ数
と
ゼータ関数

荒川恒男・伊吹山知義・金子昌信 著

牧野書店

まえがき

この本は，数学のいろいろな場面で登場する「ベルヌーイ数」と呼ばれる一連の有理数と，それに関係する，整数論で非常に重要な「ゼータ関数」という関数について，アマチュア数学愛好家にもプロの研究者にも，ともに楽しく読んでいただけるようにと願って執筆されました．やさしい部分も難しい部分もありますが，読者の好みに応じて，この魅力的な題材のどこかは楽しんでいただけるものと信じています．全体として，前から順に読まなければわからなくなるといった直線的な論理進行ではないので，各人の興味と予備知識に応じて特定の章だけ読まれてもそれぞれの面白さがあるものと思います．いままで，正面きってベルヌーイ数のみについて書かれた本はあまりなかったように思います．この本の内容はある意味で比較的スタンダードな整数論入門の部分も多いのですが，切り口はそれほどスタンダードでないところもありますし，実はいままでどの本にも書かれたことのなかった新しい部分も入っています．

さて，世の中に名前のついた数は数多くありますが，ベルヌーイ数とは一体何でしょうか．高校で1からnまで加えたときの和の公式というのを習います．あるいは2乗の和，つまり$1^2+2^2+\cdots+n^2$の公式も高校の教科書にのっています．では，指数をどんどん大きくしていって，たとえば6乗の和

$$1^6+2^6+\cdots+n^6$$

の公式はどうなるのでしょうか？　このような疑問をもつ人は多いようで，元気な高校生が挑戦して答を見つけるのは，よくあることのように思います．実は，この答は，6乗と限らず任意のべきについて，少なくとも18世紀はじめごろには知られていました．（答は2ページを見てください．）ベルヌーイはこのような公式をつくるために特別な数を導入しました．これがベルヌーイ数です．（詳しい歴史は第1章を見てください．）本書では，いろいろなところにこの「べき乗和」の公式がでてきます．実は，本書では「べき乗和」の公式は都合4回も別々の証明が与えられます．（第1章1.2節，第4章注意4.10，第5章

注意 5.6，および第 8 章補題 8.11 です.）

しかし，べき乗和の公式がそんなに面白いのでしょうか．面白いには違いないのですが，もしベルヌーイ数の価値がこれだけだったらこれで 1 冊の本を書くことはなかったでしょう．ベルヌーイ数の真価は少し違ったところにあります．次の公式の例を見てください．

$$1+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\frac{1}{5^2}+\frac{1}{6^2}+\cdots=\frac{\pi^2}{6},$$
$$1+\frac{1}{2^4}+\frac{1}{3^4}+\frac{1}{4^4}+\frac{1}{5^4}+\frac{1}{6^4}+\cdots=\frac{\pi^4}{90},$$
$$1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+\frac{1}{9}-\frac{1}{11}+\cdots=\frac{\pi}{4}.$$

（証明は 61 ページ系 4.12 と 148 ページ定理 9.6 にあります.） こういう式ははじめて見ると非常に神秘的な感じがするように思います．単純な有理数の規則正しい和が，円周率という超越的な数に突然化けてしまうのですから．これらの式の左辺は，本書で登場する，もう 1 つの重要な対象，つまりゼータ関数とか L 関数とかいわれる関数の特殊な点での値です．ゼータ関数というのはたとえば

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}=1+\frac{1}{2^s}+\frac{1}{3^s}+\frac{1}{4^s}+\frac{1}{5^s}+\frac{1}{6^s}+\cdots$$

のような，変数 s に関する関数のことです．特にこの関数 $\zeta(s)$ のことをリーマンゼータ関数といいます．前の例の最初の 2 つの式の左辺は $\zeta(s)$ の $s=2$ と $s=4$ における値，つまり $\zeta(2)$ と $\zeta(4)$ です．右辺はベルヌーイ数，ないしは一般ベルヌーイ数と呼ばれる数が関係しています．実はベルヌーイ数が整数論にとって欠くことができない存在なのは，ここで述べたような，ゼータ関数の特殊値（特殊な点での値）との関係にその理由があります．ゼータ関数という名前のついた関数は整数論の世界に山ほど登場しますし，いつも非常に重要な情報を含んでいます．1 つひとつの重要な整数論的対象ごとに，1 つひとつ別なゼータが現れるといってもいいほどです．ベルヌーイ数と関係するゼータ関数はその中のほんの一部にすぎません．しかしそれでも非常にたくさんの整数論的な現象と関係しています．たとえば非ユークリッド幾何学のある種の体積に現れたり，保型形式と呼ばれる関数の空間の次元公式や 2 次形式の同値類の個

数（類数）の公式に現れたり，アイゼンシュタイン級数という大切な関数の定数項に現れたり．そのほか，1 のべき根を有理数につけ加えた数の体系（円分体）の整数論とも関係があります．こういった理論を全面的に説明するためには，それだけで新しい本が必要になりますから，本書で説明するのは無理です．しかし，関係のヒントは与えるように努めました．

以下，読者の便宜のために，各章の内容について，簡単に述べます．括弧の中に書いたことは，この本では説明していないこともあります．

第 1 章では，そもそものベルヌーイ数の導入の歴史と，漸化式によるベルヌーイ数の定義ののちにべき乗和の公式が証明されます．またベルヌーイ数の母関数によるもっとわかりやすい定義も与えられます．第 2 章でベルヌーイ数を簡単に書く 1 つの公式を与えます．スターリング数という定義の比較的単純な数を用いて書きます．第 3 章ではベルヌーイ数の分母を調べるクラウゼン・フォンシュタウトの定理と，ベルヌーイ数どうしの間で成り立つ合同式であるクンマー合同式を述べます．（これは p 進ゼータ関数というものを定義するときに必要です．） 第 4 章では，ベルヌーイ数を拡張してディリクレ指標つきの一般ベルヌーイ数を定義します．（こうすることにより，2 次体や円分体との結びつきがでてきます．） またベルヌーイ多項式（その母関数がベルヌーイ数のときと非常に似ている多項式系）が一般ベルヌーイ数との関係で定義され，その応用として，べき乗和の公式の 2 つ目の証明が得られます．また，リーマンゼータ関数の正の偶数での値をベルヌーイ数で表す公式も得られます．第 5 章では関数の整数点での和を評価するのに非常に有用なオイラー・マクローリンの定理が述べられます．評価の公式の係数にベルヌーイ数やベルヌーイ多項式がでてきます．この応用として，リーマンゼータ関数の解析接続が示され，ゼータ関数の 0 以下の整数での値がベルヌーイ数を用いて綺麗に表示されます．第 6 章では 2 次体のイデアルと 2 次形式の関係を述べ，一般ベルヌーイ数と正定値 2 次形式の類数の関係が述べられます．第 7 章では虚 2 次体の類数と普通の（指標のつかない）ベルヌーイ数の合同関係式が示されます．第 8 章ではまずガウス和について説明し，1 のべき根に指標をつけてとったさまざまな和をガウス和と一般ベルヌーイ数で記述するいろいろな公式を与えます．ここでべき乗和の公式の 3 番目の証明が得られます．第 9 章ではゼータ関数の定義を指標をつけて

少しかえた L 関数を定義し，コンタワー積分表示というものを用いて関数等式を示すとともに，この関数の 0 以下の整数での値が一般ベルヌーイ数で記述できるという公式を示します．実はこれが一般ベルヌーイ数の大きな意義といえます．第 10 章では概均質ベクトル空間のゼータ関数のうちで，外見からまったく明らかというわけではないが，実はやさしい関数になっている例をあげます．(これは保型形式の次元公式にベルヌーイ数が現れる例になっています.）第 11 章ではクンマー合同式を p 進測度を考えることにより再度証明します．(p 進 L 関数と深い関係があります.）第 12 章では,（コ）タンジェントの展開係数にベルヌーイ数がでてくるが，これを楕円関数で置き換えたらどうなるか（三角関数についての現象を一般化するときの常套手段!）という，フルヴィッツ数の理論を説明します．第 13 章では，フルヴィッツゼータ関数の一般化の一種であるバーンズの多重ゼータ関数の解析接続と，その特殊値とベルヌーイ多項式との関係，および 2 重ゼータ関数の関数等式（第 9 章と同様の方法）が述べられます．第 14 章では普通のベルヌーイ数の母関数を，多重対数関数というものを用いて一般化することで定義される，多重ベルヌーイ数について説明されます．

以上のように多くの現象と関係しているベルヌーイ数ですが，ベルヌーイ数固有の研究課題というものは（非常に難しい未解決問題もあるにはあるのですが）あまりなく，おそらくベルヌーイ数のみを専門に研究している数学者というものは，ほとんど存在しないでしょう．それだけにいままで類書が存在せず，ベルヌーイ数の多岐にわたる関係を概観するのが，あまり容易でない面もあったように思います．筆者たちも整数論の専門家ではありますが，特にベルヌーイ数が専門というわけではありません．本書は，筆者たちが，ほかの興味から折に触れベルヌーイ数とかかわってきたことについて，自分たちの論文から引用した部分もあるけれど，他の部分では一種の備忘録（つまり必ずしも論文に書くようなことでもないけれど，ちょっと調べたことや，気がついた解釈や計算などを忘れないように書き留めたもの）という側面があるといえなくもありません．そしてこのようなかかわり方が，実はベルヌーイ数への比較的普通のかかわり方ではないかと考えます．この意味で，本書は十分読者のお役に立つであろうと信じます．

なお，最後に,「ベルヌーイ数」という魅力的なテーマを提案され，本書の執

筆をお勧めくださった，牧野書店の牧野末喜氏に深く感謝したいと思います．実際，本書の執筆は，同氏より著者のひとり，伊吹山知義に具体的にこのテーマでの執筆をお勧めをいただき，伊吹山が研究者仲間の荒川恒男，金子昌信に共同執筆を提案する形でスタートしました．同氏のお勧めがなければ，このような本を完成させることはなかったであろうと思います．

また，原稿を通読して多くのコメントを下さった落合啓之氏にも心から感謝いたします．

2000 年 12 月

著者しるす

目　次

第1章

ベルヌーイ数

1.1 定義——歴史からの導入

ベルヌーイ数がはじめて世にでたのは，Jakob Bernoulli[1]の遺著 *Ars Conjectandi*[2]において，1713年のことであるといわれている．彼はそこで自然数のべき乗の和 $1^k+2^k+\cdots+n^k$ の公式，つまり

$$\sum_{i=1}^{n} i=\frac{n(n+1)}{2},\quad \sum_{i=1}^{n} i^2=\frac{n(n+1)(2n+1)}{6},\quad \sum_{i=1}^{n} i^3=\left(\frac{n(n+1)}{2}\right)^2,\cdots$$

などを10乗 $(k=10)$ まで表にした後[3]，一般の場合の公式をいわゆるベルヌーイ数を用いて与え，そのベルヌーイ数がどのようにして決まる数であるかを説明している．Bernoulli はこの公式がべき乗和の計算にいかに有効であるかを強調し，自身がこれを用いて1から1000までの10乗の和[4]を計算するのに「4分の1時間の半分」もかからなかったと述べている．

その一般公式を現代の記法で書くと，

---

[1] 1654.12.27 スイス Basel 生——1705.8.16 スイス Basel 没. Jakob は，英 James，仏 Jacques. 有名な Bernoulli 一家の数学者の中で一番の年長. 弟 Johann（1667.7.27 スイス Basel 生——1748.1.1 スイス Basel 没），その次男 Daniel（1700.2.8 オランダ Groningen 生——1782.3.17 スイス Basel 没）の3人が特に優れていたといわれる.

[2] ラテン語. ars は「術」「方法」などの意. conjectandi は「推測する」の意の動詞 conjecto の動名詞. 確率論における，Bernoulli の大数の法則はこの本で述べられた.

[3] Bernoulli は右辺を因数分解しない形で書いている．また，9乗の和の公式の n^2 の係数が違っている.

[4] 正しく値 91409924241424243424241924242500 が記されている.

$$\sum_{i=1}^{n} i^k = \sum_{j=0}^{k} \binom{k}{j} B_j \frac{n^{k+1-j}}{k+1-j} \tag{1.1}$$

となる．ここに $\binom{k}{j}$ は2項係数

$$\binom{k}{j} = \frac{k(k-1)(k-2)\cdots(k-j+1)}{j!}$$

で，B_j は漸化式

$$\sum_{j=0}^{k} \binom{k+1}{j} B_j = k+1 \qquad (k=0,1,2,\cdots)$$

により定まる数である．この B_j がのちにベルヌーイ数と呼ばれることになった数であって[5]，この本の主題である．

Bernoulli は B_0 と B_1 の項にははじめから数をあてて記号をつけておらず，B_2 以降の偶数番目のみ A, B, C, D などと記している[6]．

ところが，わが国においても，*Ars Conjectandi* 出版の前年 1712 年[7]に出版の，和算家 関孝和[8]の遺稿集『括要算法』において，やはりべき乗和の公式とベルヌーイ数の漸化的な定義が与えられている．すなわち『括要算法』巻元（第1巻のこと），垜積術解[9]の章，方垜の項において，まず例題として1から3までの各べき乗の和の求め方を11乗まで述べた後，一般の n までの和を求めるアルゴリズムを解説し，そうして B_{11} までの計算と表，11乗までのべき乗和の公式の表を正しく与えている．

関が与えたべき乗和の公式も B_j を求めるアルゴリズムも Bernoulli のものと

---

[5]ベルヌーイ数と命名したのは de Moivre（Abraham, 1667.5.26 フランス Vitry 生 ——1754.11.27 イギリス London 没），*Miscellanea analytica de seriebus et quadraturis*（London, 1730）という本においてらしい．de Moivre はドモアブルの定理で有名．

[6]奇数番目は B_1 以外は0となる（後述）．Bernoulli の本で (1.1) の右辺は（$k=c$）

$$\frac{1}{c+1}n^{c+1} + \frac{1}{2}n^c + \frac{c}{2}An^{c-1} + \frac{c.c-1.c-2}{2.3.4}Bn^{c-3} + \frac{c.c-1.c-2.c-3.c-4}{2.3.4.5.6}Cn^{c-5}$$
$$+\frac{c.c-1.c-2.c-3.c-4.c-5.c-6}{2.3.4.5.6.7.8}Dn^{c-7} + \cdots$$

と書かれている．

[7]正徳2年．この前後の元号は，元禄，宝永，正徳，享保と続いている．

[8]1642.3（異説あり 1637 とも）上野の国藤岡生（江戸小石川の説も）——1708.10.24 江戸没

[9]垜は「だ」と読む．辞書に「あづち．弓の的を立てかけておく築地（ついじ）.」とある．べき乗和のことを「方垜」と称している．

まったく同じであり，関は $B_0, B_1, B_2, \cdots$ を順に一級，二級，三級，$\cdots$ の「取数」と名づけている[10].

関の原本は漢文と独特の記法（算木）で書かれており読みやすくはないが[11]，幸い『関孝和全集』[74] は巻末に解説が付され，しかもその英訳もついている．関孝和が Bernoulli とは独立にベルヌーイ数を発見していたことは [34, 35] や [66] などにも紹介されているが，残念ながら Bernoulli ほどには知られていないように思われる．

こうした事実から，ベルヌーイ数は「関・ベルヌーイ数」と呼ばれるべきものと思われるが，ここは慣習に従ってこの本でも単にベルヌーイ数ということにする．

関も Bernoulli も公式 (1.1) の導き方については多くを述べていないのであるが，そもそもこのべき乗和の公式を論じたのは関や Bernoulli がはじめてではない．Bernoulli の著 *Ars Conjectandi* にも名前があげられているが，Faulhaber[12]は彼らに先立つこと約 80 年，1631 年に出版の著書 *Academia Algebrae* において，k が奇数のときの $\sum_{i=1}^{n} i^k$ は $\frac{n(n+1)}{2} = \sum_{i=1}^{n} i$ の多項式で書けること（$\sum_{i=1}^{n} i^3 = \left(\sum_{i=1}^{n} i\right)^2$ がその最初の例），また k が偶数のときは，$\sum_{i=1}^{n} i^k$ は n の多項式として $\frac{n(n+1)(2n+1)}{6} = \sum_{i=1}^{n} i^2$ で割れて，その商がまた $\sum_{i=1}^{n} i$ の多項式で書けることを述べ，その多項式の係数を求める方法も与えているらしい．ただし，ベルヌーイ数の発見にはいたらなかったようである．上の事実は後に Jacobi[13]が再発見，厳密な証明を与えた（[46]）．次節で，公式 (1.1) の 1 つの導き方を述べる．Faulhaber の結果については紹介するにとどめ，証明は文献に譲ることとした．

さてここで改めてベルヌーイ数の定義を与えよう．ここでは関と Bernoulli による漸化的な定義を採用するとし，ベルヌーイ数の母関数表示は後に与える．次節で示すように両者は同値であって，母関数表示のほうを定義に採用すること

---

[10] Bernoulli と違って，B_0, B_1 および 0 となる奇数番目の B_n も同列に扱っている．

[11] Bernoulli の原著もラテン語で現代のわれわれには近づきにくいが，少なくとも数式を読み取るのに苦労はいらない．

[12] Johann Faulhaber（1580.5.5 ドイツ Ulm 生——1635 ドイツ Ulm 没）

[13] Carl Gustav Jacob Jacobi （1804.12.10 ドイツ Potsdam 生——1851.2.18 ドイツ Berlin 没）

も多い．

定義 1.1　ベルヌーイ数 B_n $(n=0,1,2,\cdots)$ を逐次

$$\sum_{i=0}^{n}\binom{n+1}{i}B_i=n+1 \qquad (n=0,1,2,\cdots) \tag{1.2}$$

で定める．

小さな n について順に B_n を計算してみよう．まず $n=0$ として

$$B_0=1.$$

これと，$n=1$ のときの

$$B_0+2B_1=2$$

より

$$B_1=\frac{1}{2}(2-B_0)=\frac{1}{2}.$$

これらと $n=2$ のときの

$$B_0+3B_1+3B_2=3$$

より

$$B_2=\frac{1}{3}(3-B_0-3B_1)=\frac{1}{6}.$$

以下同様に，$n=3$ のときの

$$B_0+4B_1+6B_2+4B_3=4$$

より

$$B_3=\frac{1}{4}(4-B_0-4B_1-6B_2)=0.$$

$n=4$ のときの

$$B_0+5B_1+10B_2+10B_3+5B_4=5$$

より

$$B_4=\frac{1}{5}(5-B_0-5B_1-10B_2-10B_3)=-\frac{1}{30}$$

などとなっている．さらに少し先までの値を表にしておく．定義から明らかなように，B_n は有理数である．現在では Mathematica や Maple などの数式処理ソフトにベルヌーイ数が組み込み関数として入っていて，（機械にもよろうが）

はじめの数百番目程度までの具体的な値は難なくわかる．

表 1.1: ベルヌーイ数

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
B_n	1	$\frac{1}{2}$	$\frac{1}{6}$	0	$-\frac{1}{30}$	0	$\frac{1}{42}$	0	$-\frac{1}{30}$	0	$\frac{5}{66}$	0	$-\frac{691}{2730}$	0	$\frac{7}{6}$

注意 1.2 現今最も多く見られるベルヌーイ数の定義には，奇数番目を飛ばすものを別とすれば，上の定義と B_1 の符号だけが異なるもの（すなわち $B_1 = -\frac{1}{2}$ で他は同じ）が採用されることが多い[14]．しかし，関や Bernoulli のオリジナルな定義が上のものであること，また後に述べるリーマンゼータ関数の特殊値との関係に鑑みて，あえてこの定義を採用することにした[15]．違いは些細であるものの，注意をお願いしたい．

なお，n が 3 以上の奇数のとき $B_n = 0$ であること（後で証明する）より，どちらの定義を採用しても B_n を $(-1)^n B_n$ に置き換えることで他方に移る．したがってすべての公式を読み替えるのは容易であることも注意しておく．

1.2 べき乗和の公式とファウルハーバーの定理

以下において，

$$S_k(n) := \sum_{i=1}^{n} i^k \quad (k \geq 0, n \geq 1,\ \text{ともに整数})$$

の関・ベルヌーイの公式 (1.1) の証明を与える．そのあとファウルハーバーの定理を述べ，節の最後にベルヌーイ数のある漸化式を与える．

証明に入る前に，$S_k(n)$ の具体式をいくつか与えておこう．

---

[14] それを (1.2) と似た漸化式で定義しようとすると，$B_0 = 1$ と $\sum_{i=0}^{n} \binom{n+1}{i} B_i = 0$ $(n \geq 1)$ とに分ける必要がある．

[15] これは，やはり日本の偉大な数学者である岩澤健吉（1917.9.11 群馬生——1998.10.26 東京没）が採用した定義（[45]）を踏襲することにもなる．

$$
\begin{aligned}
S_0(n) &= n,\\
S_1(n) &= \frac{n^2}{2} + \frac{n}{2}\\
&= \frac{1}{2}n(n+1),\\
S_2(n) &= \frac{n^3}{3} + \frac{n^2}{2} + \frac{n}{6}\\
&= \frac{1}{6}n(n+1)(2n+1),\\
S_3(n) &= \frac{n^4}{4} + \frac{n^3}{2} + \frac{n^2}{4}\\
&= \frac{1}{4}n^2(n+1)^2,\\
S_4(n) &= \frac{n^5}{5} + \frac{n^4}{2} + \frac{n^3}{3} - \frac{n}{30}\\
&= \frac{1}{30}n(n+1)(2n+1)(3n^2+3n-1),\\
S_5(n) &= \frac{n^6}{6} + \frac{n^5}{2} + \frac{5n^4}{12} - \frac{n^2}{12}\\
&= \frac{1}{12}n^2(n+1)^2(2n^2+2n-1),\\
S_6(n) &= \frac{n^7}{7} + \frac{n^6}{2} + \frac{n^5}{2} - \frac{n^3}{6} + \frac{n}{42}\\
&= \frac{1}{42}n(n+1)(2n+1)(3n^4+6n^3-3n+1).
\end{aligned}
$$

証明であるが，まず，

$$S_0(n) = n$$

は自明である．$k \geq 1$ とする．2 項展開により得られる式

$$(m+1)^{k+1} - m^{k+1} = \sum_{j=0}^{k} \binom{k+1}{j} m^j$$

において，$m = 1, 2, \cdots, n$ としたものを辺々加えると

$$(n+1)^{k+1} - 1 = \sum_{j=0}^{k} \binom{k+1}{j} S_j(n)$$

を得る．これより，

$$S_k(n) = \frac{1}{k+1}\left\{(n+1)^{k+1} - 1 - \sum_{j=0}^{k-1} \binom{k+1}{j} S_j(n)\right\}.$$

この式で $k=1,2,\cdots$ としていくと順に

$$S_1(n)=\frac{n^2}{2}+\frac{n}{2},\ S_2(n)=\frac{n^3}{3}+\frac{n^2}{2}+\frac{n}{6},\cdots$$

と求まっていき，帰納的に，

$$S_k(n)\ \text{は}\ \frac{1}{k+1}n^{k+1}\ \text{で始まる}\ n\ \text{の}\ k+1\ \text{次多項式である}$$

ことがわかる．この多項式をより具体的に求めるのが目標である．

そこで，その多項式を，x を変数として $S_k(x)\ (=\frac{1}{k+1}x^{k+1}+\cdots)$ と書く．一般に，「2 つの多項式 $f(x),g(x)$ について，$f(n)=g(n)$ がすべての自然数 n について成り立つならば恒等的に $f(x)=g(x)$ である」ことに注意すると，定義から

$$S_k(n+1)-S_k(n)=(n+1)^k \qquad (n=1,2,3,\cdots)$$

であるから，

$$S_k(x+1)-S_k(x)=(x+1)^k$$

が成り立つ．ここで $x=0$ とおいて $S_k(1)=1$ を用いると，

$$S_k(0)=0.$$

これで $S_k(x)$ の定数項と最高次係数がわかった．あとの係数は微分係数 $S_k^{(j)}(0)$, $1\le j\le k$ がわかればよい．そこで，上式を微分した式

$$S'_k(x+1)-S'_k(x)=k(x+1)^{k-1} \tag{1.3}$$

で $x=0,1,2,\cdots,n-1$ とおいて足すと

$$S'_k(n)-S'_k(0)=kS_{k-1}(n).$$

これが任意の自然数 n について成り立つので，$S'_k(0)=b_k$ とおくと $(b_0=1)$,

$$S'_k(x)=kS_{k-1}(x)+b_k$$

が多項式の間の関係として成り立つ．これを微分すると

$$S''_k(x)=kS'_{k-1}(x), \tag{1.4}$$

$x=0$ とおいて

$$S''_k(0)=kb_{k-1}.$$

(1.4) 式をさらに微分して，k を $k-1$ にした式を使うと

$$S'''_k(x)=kS''_{k-1}(x)=k(k-1)S'_{k-2}(x).$$

ここで $x=0$ とおいて

$$S_k'''(0) = k(k-1)b_{k-2}.$$

以下同様に次々と微分していって，

$$S_k^{(j)}(0) = k(k-1)\cdots(k-j+2)b_{k-j+1} \qquad (2 \leq j \leq k+1)$$

を得る．したがって，

$$\begin{aligned} S_k(x) &= \sum_{j=0}^{k+1} \frac{S_k^{(j)}(0)}{j!} x^j \\ &= \sum_{j=1}^{k+1} \frac{1}{k+1} \binom{k+1}{j} b_{k-j+1} x^j \qquad (S_k^{(0)}(0) = 0) \\ &= \frac{1}{k+1} \sum_{j=0}^{k} \binom{k+1}{j} b_j x^{k+1-j}. \end{aligned}$$

$S_k(1) = 1$ であるから，この式で $x = 1$ とすれば

$$k+1 = \sum_{j=0}^{k} \binom{k+1}{j} b_j.$$

これはまさにベルヌーイ数の満たす漸化式にほかならない．すなわち $b_j = B_j$ である．等式

$$\frac{1}{k+1}\binom{k+1}{j} = \frac{1}{k+1-j}\binom{k}{j}$$

に注意すれば，これより公式 (1.1) が従う． ∎

注意 1.3　$S_k'(x-1) = B_k(x)$ とおくと（$B_k(x) = x^k + \cdots$），(1.3), (1.4) 式より

$$B_k(x+1) - B_k(x) = kx^{k-1}, \qquad B_k'(x) = kB_{k-1}(x)$$

が成り立つ．この $B_k(x)$ がベルヌーイ多項式と呼ばれるもので，さまざまな応用がある．定義といくつかの性質が 4.3 節（55 ページ）において述べられる．べき乗和の公式もベルヌーイ多項式の性質から簡単に導くことができ，それも 4.3 節で与える．

多項式 $S_k(x)$ を用いて，k が 3 以上の奇数のときの B_k が 0 になることを証明しておこう．これは後で母関数を使って簡単に証明するが，それ以前に使うのでここでも示しておく．

命題 1.4　n を 3 以上の奇数とするとき $B_n = 0$. したがって $n \neq 1$ なるすべての整数 $n \geq 0$ に対し $(-1)^n B_n = B_n$.

証明　$k \geq 1$ とする．$S_k(x+1) - S_k(x) = (x+1)^k$ において $x = -1$ とおいて $S_k(0) = 0$ を使うと $S_k(-1) = 0$. そこで，上記証明中で得られている $S_k(x)$ の公式

$$(k+1)S_k(x) = \sum_{j=0}^{k} \binom{k+1}{j} B_j x^{k+1-j}$$

において $x = -1$ とおくと

$$\sum_{j=0}^{k} \binom{k+1}{j} (-1)^j B_j = 0.$$

これと，ベルヌーイ数を定義する漸化式

$$\sum_{j=0}^{k} \binom{k+1}{j} B_j = k+1$$

との差をとると奇数番目だけが残り

$$2 \sum_{j=0}^{[\frac{k-1}{2}]} \binom{k+1}{2j+1} B_{2j+1} = k+1.$$

（$[x]$ はガウス記号，すなわち x を越えない最大の整数を表す.）左辺 $j = 0$ の項が（$B_1 = 1/2$ より）右辺と打ち消すので，

$$\sum_{j=1}^{[\frac{k-1}{2}]} \binom{k+1}{2j+1} B_{2j+1} = 0 \qquad (k \geq 3)$$

を得る．この式で $k = 3, 5, 7, \cdots$ としていくことにより順にすべての $B_k = 0$ (k : 奇数 ≥ 3) が従う. ∎

次に，ファウルハーバーの定理を述べよう.

定理 1.5　$k \geq 1$ とし，$u = n(n+1)$ $(= 2S_1(n)), v = n(n+1)(2n+1)$ $(= 6S_2(n))$ とおく．このとき，

$$S_{2k+1}(n) = \frac{u^2}{2k+2} \sum_{i=0}^{k-1} A_i^{(k)} u^{k-1-i}$$

および

$$S_{2k}(n) \doteq \frac{v}{(2k+1)(2k+2)} \sum_{i=0}^{k-1} (k+1-i) A_i^{(k)} u^{k-1-i}$$

と書かれる．ただし $A_i^{(k)}$ は

$$A_0^{(k)} = 1,\ A_i^{(k)} = -\frac{1}{k+1-i} \sum_{j=0}^{i-1} \binom{k+1-j}{k+j-2i} A_j^{(k)} \qquad (1 \leq i \leq k-1)$$

により決まる数である（$k+j-2i<0$ ならば $\binom{k+1-j}{k+j-2i}=0$ とする）．

証明は文献（[23], [53] など）に譲るが，興味のある読者は証明を試みられたい．

この節の最後に，$S_k(x)$ を用いてベルヌーイ数のある漸化式（[49]）を証明しておく．

ベルヌーイ数を定義する漸化式 (1.2) の右辺を移項し，$i \neq 1$ なら $(-1)^i B_i = B_i$ であることと $B_1 = 1/2$ を使うと，$n \geq 1$ のとき

$$\sum_{i=0}^{n} (-1)^i \binom{n+1}{i} B_i = 0 \tag{1.5}$$

が成り立つ．いま $\widetilde{B_n} = (n+1)B_n$ とおく．このとき

定理 1.6　$n \geq 1$ に対し，次式が成り立つ．

$$\sum_{i=0}^{n} (-1)^i \binom{n+1}{i} \widetilde{B_{n+i}} = 0.$$

注意 1.7　この式は (1.5) 式に非常に似ているが，$\widetilde{B_{2n}}$（したがって B_{2n}）を計算するのに半分の項しか必要としていない．

証明　2 項展開から得られる式

$$x^{n+1}(1-x)^{n+1} = \sum_{i=0}^{n+1} (-1)^i \binom{n+1}{i} x^{n+i+1}$$

の両辺を x で微分して

$$(n+1)\{x^n(1-x)^{n+1} - x^{n+1}(1-x)^n\} = \sum_{i=0}^{n+1} (-1)^i \binom{n+1}{i} (n+i+1) x^{n+i}.$$

これより

$$(n+1)x^n(1-x)^n(1-2x) = (-1)^{n+1}(2n+2)x^{2n+1} + \sum_{i=0}^{n} (-1)^i \binom{n+1}{i} (n+i+1) x^{n+i}. \tag{1.6}$$

ここで $2x-1=y$ とおくと，

$$\begin{aligned}
\text{左辺} &= -(n+1)\left(\frac{1+y}{2}\right)^n\left(\frac{1-y}{2}\right)^n y \\
&= -2^{-2n}(n+1)y(1-y^2)^n \\
&= -2^{-2n}(n+1)\sum_{i=0}^{n}(-1)^i\binom{n}{i}y^{2i+1}.
\end{aligned}$$

いま，

$$\sum_{x=1}^{m} y^{2i+1} = \sum_{x=1}^{m}(2x-1)^{2i+1} = S_{2i+1}(2m) - 2^{2i+1}S_{2i+1}(m)$$

であるので，(1.6) 式において $x = 1, 2, \cdots, m$ として足すと

$$\begin{aligned}
&-2^{-2n}(n+1)\sum_{i=0}^{n}(-1)^i\binom{n}{i}\left(S_{2i+1}(2m) - 2^{2i+1}S_{2i+1}(m)\right) \\
&\quad= (-1)^{n+1}(2n+2)S_{2n+1}(m) + \sum_{i=0}^{n}(-1)^i\binom{n+1}{i}(n+i+1)S_{n+i}(m).
\end{aligned}$$

これがすべての自然数 m について成り立つので，何度か使った論法により，m を x にかえて，

$$\begin{aligned}
&-2^{-2n}(n+1)\sum_{i=0}^{n}(-1)^i\binom{n}{i}\left(S_{2i+1}(2x) - 2^{2i+1}S_{2i+1}(x)\right) \\
&\quad= (-1)^{n+1}(2n+2)S_{2n+1}(x) + \sum_{i=0}^{n}(-1)^i\binom{n+1}{i}(n+i+1)S_{n+i}(x)
\end{aligned}$$

が多項式の関係として成り立つ．この式を x で微分して $x = 0$ とおく．$S'_k(0) = B_k$ であること（前節），また左辺で $i = 0$ の項は $2S'_1(0) - 2S'_1(0) = 0$ より消えること，および k が 3 以上の奇数のとき $B_k = 0$ となること（命題 1.4）より，求める漸化式が得られる．∎

1.3　形式的べき級数

われわれはベルヌーイ数を漸化式を用いて定義したのであるが，形式的べき級数による母関数表示

$$\frac{te^t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!} \tag{1.7}$$

によってベルヌーイ数を導入する方法もよく見られる．1.1 節注意 1.2 で触れた，B_1 の符号だけが異なる定義の場合は左辺は $\frac{t}{e^t-1}$ である．実際，母関数表示はいろいろな性質を調べるのに便利なことが多い．

そこで，以下この節で，慣れていない読者のために形式的べき級数について基本的なことを解説した後，次節で，上の等式を定理 1.12 として証明することにする．ただし，抽象代数的な記述になじみのない読者は，次節を参照しながら，あるいは先に次節でどのような計算をするのか眺めた上でこの節を読まれるとよい．

R を単位元（普通に 1 と書く）をもつ可換整域とする．（と，一般的に記述するが，この本では p 進測度を扱う第 11 章を除いて，もっぱら $R=\mathbf{Q}$（有理数体）か $\mathbf{Q}$ の有限次拡大であるし，当面 $R=\mathbf{Q}$ と思って読んでいただいてさしつかえない．可換整域とは $ab=0$ ならば $a=0$ または $b=0$ が成り立つような可換環のこと．）R に係数をもつ，不定元 t に関する形式的な式

$$\sum_{n=0}^{\infty} a_n t^n = a_0 + a_1 t + a_2 t^2 + a_3 t^3 + \cdots$$

を（R 係数の）形式的べき級数といい，その全体の集合を $R[[t]]$ で表す．2 つの形式的べき級数が等しいとは，t に関するすべての係数が一致することである．以下においてしばしば登場する形式的べき級数に

$$e^t = \sum_{n=0}^{\infty} \frac{t^n}{n!} = 1 + \frac{t}{1!} + \frac{t^2}{2!} + \frac{t^3}{3!} + \cdots$$

および

$$\log(1+t) = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{t^n}{n} = t - \frac{t^2}{2} + \frac{t^3}{3} - \cdots$$

がある．これらは，（実または複素）関数 e^x および $\log(1+x)$ を原点の周りでテイラー[16]展開して得られるべき級数を（収束云々を問題にせず）形式的な式と見たものである．変数を t にかえただけで同じ関数記号 $e^t, \log(1+t)$ を用いるが，t に値が入ることはなく，あくまで単に右辺の形式的べき級数を表すものと約束する．

2 つの形式的べき級数の和および積を

[16]Brook Taylor（1685.8.18 イギリス Edmonton 生——1731.12.29 イギリス London 没）

$$\sum_{n=0}^{\infty} a_n t^n + \sum_{n=0}^{\infty} b_n t^n = \sum_{n=0}^{\infty} (a_n + b_n) t^n$$

および

$$(\sum_{n=0}^{\infty} a_n t^n) \cdot (\sum_{n=0}^{\infty} b_n t^n) = \sum_{n=0}^{\infty} c_n t^n, \qquad c_n = \sum_{i=0}^{n} a_i b_{n-i}$$

で定義する．積は分配法則を形式的に適用する形で定義されており，最初のほうだけを取り出した形で書くと

$$\begin{aligned}
&(a_0 + a_1 t + a_2 t^2 + a_3 t^3 + \cdots) \cdot (b_0 + b_1 t + b_2 t^2 + b_3 t^3 + \cdots) \\
&\quad = a_0 b_0 + (a_0 b_1 + a_1 b_0) t + (a_0 b_2 + a_1 b_1 + a_2 b_0) t^2 \\
&\qquad\qquad + (a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0) t^3 + \cdots
\end{aligned}$$

となる．この定義によって $R[[t]]$ が可換環になることは容易に確かめることができる．加法の零元，乗法の単位元はそれぞれ

$$0 + 0 \cdot t + 0 \cdot t^2 + 0 \cdot t^3 + \cdots$$

および

$$1 + 0 \cdot t + 0 \cdot t^2 + 0 \cdot t^3 + \cdots$$

なる形式的べき級数で，それぞれ単に $0, 1$ と書く．一般に，定数項以外の係数がすべて 0 であるような形式的べき級数の全体は自然に R と同一視される．また，R 係数多項式を，有限個の n 以外はすべて $a_n = 0$ となる形式的べき級数と見なすことにより，R 係数多項式の全体のなす可換環 $R[t]$ も $R[[t]]$ の部分環と見なせる．上の $R[[t]]$ における和，積の定義は，多項式の和，積の定義をそのまま拡張したものである．

R は整域と仮定しているので $R[[t]]$ も整域となる．すなわち，

命題 1.8 $R[[t]]$ は零因子をもたない（0 でない 2 つの元の積は 0 でない）．特に，$A \neq 0,\ AB = AC \quad (A, B, C \in R[[t]])$ ならば $B = C$ である．

証明 $A = a_0 + a_1 t + a_2 t^2 + a_3 t^3 + \cdots, B = b_0 + b_1 t + b_2 t^2 + b_3 t^3 + \cdots$ がともに 0 でないとし，a_k, b_l をそれぞれの 0 ではない最初の係数とする．このとき，$A \cdot B = c_0 + c_1 t + c_2 t^2 + \cdots$ において t^{k+l} の係数

$$c_{k+l} = a_0 b_{k+l} + a_1 b_{k+l-1} + \cdots + a_k b_l + \cdots + a_{k+l-1} b_1 + a_{k+l} b_0$$

を見ると，R が整域という仮定より $a_k b_l$ は 0 でなく他の項はすべて 0 であるか

ら $c_{k+l} = a_k b_l \neq 0$. したがって $A \cdot B$ は0でない.

特に $AB = AC$ ならば $A(B - C) = 0$ であるので，$A \neq 0$ であれば $B = C$ となる. ∎

命題 1.9　$\sum_{n=0}^{\infty} a_n t^n$ が $R[[t]]$ において可逆である（乗法に関する逆元をもつこと）ための必要十分条件は，定数項 a_0 が R において可逆であることである.

証明　$\sum_{n=0}^{\infty} a_n t^n$ が可逆，すなわち $(\sum_{n=0}^{\infty} a_n t^n) \cdot (\sum_{n=0}^{\infty} b_n t^n) = 1$ なる形式的べき級数 $\sum_{n=0}^{\infty} b_n t^n$ が存在すれば，定数項を比べて $a_0 b_0 = 1$ であるので，a_0 は R の可逆元である.

逆に，a_0 が R の可逆元であるとする．このとき，$b_0 = a_0^{-1}$, $b_n = -a_0^{-1} \cdot \sum_{i=1}^{n} a_i b_{n-i}$ $(n \geq 1)$ によって $b_n \in R$ $(n \geq 0)$ を定めることができて，積 $(\sum_{n=0}^{\infty} a_n t^n) \cdot (\sum_{n=0}^{\infty} b_n t^n)$ を計算すると，$a_0 b_0 = 1$ かつ $n \geq 1$ のとき $\sum_{i=0}^{n} a_i b_{n-i} = 0$ だから，定義よりこの積は1に等しい．つまり $\sum_{n=0}^{\infty} b_n t^n$ が $\sum_{n=0}^{\infty} a_n t^n$ の乗法逆元である. ∎

形式的べき級数 $A(t)$ の定数項を簡単のため $A(0)$ で表すことにする．形式的べき級数は関数ではないのであくまで t のところに値が入ることはないが，0の代入だけは常に意味をもつので，この場合だけ例外的にこの記法を用いる.

次に，ある条件のもとで $R[[t]]$ の元の無限和を考えることができることを説明しよう[17]．いま，$\{A_k(t)\}_{k=1}^{\infty}$，$A_k(t) = \sum_{i=0}^{\infty} a_i^{(k)} t^i$ を形式的べき級数の無限族とする．これらが，

各 i について，$a_i^{(k)} \neq 0$ となる k は有限個

という条件を満たすとする．つまり $A_k(t) = a_{n_k}^{(k)} t^{n_k} +$(より高次の項)　$(a_{n_k}^{(k)} \neq 0)$ と書けるとき，$k \to \infty$ ならば $n_k \to \infty$ であるとする．このとき $A_1 + A_2 + A_3 + \cdots$ を

$$A_1 + A_2 + A_3 + \cdots = \sum_{i=0}^{\infty} a_i t^i,$$

ここに

$$a_i = \sum_{k=1}^{\infty} a_i^{(k)}$$

---

[17] イデアル $I = tR[[t]]$ のべきによって位相を入れ，それについて極限を考えるということであるが，ここでは位相を持ち出さないことにする.

で定義する．つまり形式的には各係数ごとの和をとるのであるが，条件よりこれがすべて有限和となるのである．

これの特別な場合として，定数項が 0 である形式的べき級数を別の形式的べき級数に「代入」するという操作がある．すなわち，$A(t)=\sum_{i=0}^{\infty} a_i t^i, B(t)=\sum_{i=1}^{\infty} b_i t^i$ $(B(0)=b_0=0)$ とするとき，

$$A(B(t))=\sum_{i=0}^{\infty} a_i (B(t))^i$$

が意味をもつ．なぜならば，$b_0=0$ ということから，$a_i(B(t))^i$ は少なくとも i 次の項から始まり，族 $\left\{a_i(B(t))^i\right\}_{i=0}^{\infty}$ は上の条件を満たすからである．簡単な例として

$$\begin{aligned} e^{-t} &= 1+\frac{(-t)}{1!}+\frac{(-t)^2}{2!}+\frac{(-t)^3}{3!}+\cdots \\ &= 1-\frac{t}{1!}+\frac{t^2}{2!}-\frac{t^3}{3!}+\cdots \end{aligned}$$

や

$$\begin{aligned} \log(1-t) = \log(1+(-t)) &= (-t)-\frac{(-t)^2}{2}+\frac{(-t)^3}{3}-\cdots \\ &= -t-\frac{t^2}{2}-\frac{t^3}{3}-\cdots \end{aligned}$$

があるが，等式

$$e^{\log(1+t)}=1+t$$

や

$$\log(1+(e^t-1))=t$$

なども形式的べき級数を代入して得られる等式として成立する．(証明を 32 ページ注意 2.7 の後で与える．)

また，定数項が 1 であるような形式的べき級数の逆元の計算も「代入」によってなされる．まず，$1-t$ の逆元は $1+t+t^2+\cdots$ であることに注意する．すなわち

$$\frac{1}{1-t}=1+t+t^2+\cdots .$$

これは積 $(1-t)(1+t+t^2+\cdots)$ を定義どおり計算してみればわかる．そこで，1 で始まるべき級数を $1+B(t)$ と書くと，$B(t)$ は定数項をもたない形式的べき

級数 $(B(0)=0)$ であり，$1+B(t)$ の逆元は

$$\frac{1}{1+B(t)}=\frac{1}{1-(-B(t))}=1+(-B(t))+(-B(t))^2+\cdots$$

で計算される．たとえば，(1.7) 式によってベルヌーイ数の最初の数項をこの計算で求めてみる．

$$\begin{aligned}e^t-1&=t+\frac{t^2}{2!}+\frac{t^3}{3!}+\frac{t^4}{4!}+\frac{t^5}{5!}+\cdots\\&=t\left(1+\frac{t}{2}+\frac{t^2}{6}+\frac{t^3}{24}+\frac{t^4}{120}+\cdots\right)\end{aligned}$$

なので，まず

$$\begin{aligned}\frac{1}{\left(1+\frac{t}{2}+\frac{t^2}{6}+\frac{t^3}{24}+\frac{t^4}{120}+\cdots\right)}&=1-\left(\frac{t}{2}+\frac{t^2}{6}+\frac{t^3}{24}+\frac{t^4}{120}+\cdots\right)\\&\quad+\left(\frac{t}{2}+\frac{t^2}{6}+\frac{t^3}{24}+\frac{t^4}{120}+\cdots\right)^2\\&\quad-\left(\frac{t}{2}+\frac{t^2}{6}+\frac{t^3}{24}+\frac{t^4}{120}+\cdots\right)^3\\&\quad+\left(\frac{t}{2}+\frac{t^2}{6}+\frac{t^3}{24}+\frac{t^4}{120}+\cdots\right)^4+\cdots\\&=1-\frac{t}{2}+\frac{t^2}{12}+0\cdot t^3-\frac{t^4}{720}+\cdots.\end{aligned}$$

これより，

$$\begin{aligned}\frac{te^t}{e^t-1}&=e^t\cdot\frac{1}{\left(1+\frac{t}{2}+\frac{t^2}{6}+\frac{t^3}{24}+\frac{t^4}{120}+\cdots\right)}\\&=\left(1+t+\frac{t^2}{2}+\frac{t^3}{6}+\frac{t^4}{24}+\cdots\right)\left(1-\frac{t}{2}+\frac{t^2}{12}+0\cdot t^3-\frac{t^4}{720}+\cdots\right)\\&=1+\frac{t}{2}+\frac{t^2}{12}+0\cdot t^3-\frac{t^4}{720}+\cdots.\end{aligned}$$

したがって，$B_0=1, B_1=\frac{1}{2}, B_2=\frac{1}{6}, B_3=0, B_4=-\frac{1}{30},\cdots$.

さて，この「代入演算」において t は単位元に相当するものだが，「逆元」については次がいえる．

命題 1.10　形式的べき級数 $A(t)=a_0+a_1t+a_2t^2+\cdots$ に対して

$$B(0)=0, \qquad A(B(t))=t$$

を満たすような形式的べき級数 $B(t)$ が存在するための必要十分条件は

$$a_0=0 \text{ かつ } a_1 \text{ が可逆}$$

なることである．このとき $B(t)$ は一意的に定まり，$B(A(t))=t$ を満たす．すなわち $A(t), B(t)$ は代入演算に関して互いに他の逆元である．

証明 $B(t)=b_1t+b_2t^2+\cdots$ が存在して $A(B(t))=t$ を満たせば，両辺の定数項および 1 次の項を比べて $a_0=0, a_1b_1=1$ となるから，条件が必要であることがわかる．

逆に，$A(t)$ が条件 $a_0=0$ かつ a_1 が可逆，を満たしているとし，$A(B(t))=t$ を満たすような $B(t)=b_1t+b_2t^2+b_3t^3+\cdots$ の係数を決めていくことを考える．このときまず $A(B(t))=t$ の t の係数から $a_1b_1=1$ でなければならないが，a_1 が可逆であるから $b_1=a_1^{-1}$ として定めることができる．$n\geq 2$ に対して，$A(B(t))$ の t^n の係数は

$$a_1(B(t))+a_2(B(t))^2+a_3(B(t))^3+\cdots+a_n(B(t))^n$$

の t^n の係数に等しく（$B(0)=0$ であるからこれより先から t^n の項は出ない），それは

$$a_1b_n+(a_2,a_3,\cdots,a_n,b_1,b_2,\cdots,b_{n-1}\text{の多項式})$$

という形に書かれる．$b_1,b_2,\cdots,b_{n-1}$ がすでに定まったものとすれば，この式 $=0$ ということと，a_1 が可逆ということから b_n を一意的に定めることができる．これより $B(t)$ の存在と，一意性もいえたことになる．

このように得られる $B(t)$ は $B(0)=0$ かつ b_1 は可逆，を満たしているので，上に証明したことより，ある $C(t)$ $(C(0)=0)$ が存在して

$$B(C(t))=t$$

となる．このとき，$t=A(B(t))$ に $C(t)$ を代入して $B(C(t))=t$ を使うと

$$C(t)=A(B(C(t)))=A(t)$$

となる．したがって

$$B(A(t))=t$$

である． ∎

前述の式

$$e^{\log(1+t)}-1=t \quad \text{あるいは} \quad \log(1+(e^t-1))=t$$

は，$\log(1+t)$ と e^t-1 が代入に関して互いに逆元であることをいっていることになる．

形式的べき級数 $\sum_{n=0}^{\infty} a_n t^n$ の微分 $\frac{d}{dt}\left(\sum_{n=0}^{\infty} a_n t^n\right)$（これを $\left(\sum_{n=0}^{\infty} a_n t^n\right)'$ とも書く）を，形式的な項別微分で

$$\frac{d}{dt}\left(\sum_{n=0}^{\infty} a_n t^n\right) = \sum_{n=1}^{\infty} n a_n t^{n-1} = a_1 + 2a_2 t + 3a_3 t^2 + 4a_4 t^3 + \cdots$$

と定める．たとえば $(e^t)' = e^t$, $(\log(1+t))' = 1 - t + t^2 - t^3 + \cdots = \frac{1}{1+t}$ など．これは和，積に関して通常の微分規則を満たす．積の微分公式 $(f(t)g(t))' = f'(t)g(t) + f(t)g'(t)$ の証明を与えておく．$f(t) = \sum_{n=0}^{\infty} a_n t^n$, $g(t) = \sum_{n=0}^{\infty} b_n t^n$ とおくと

$$\begin{aligned}
(f(t)g(t))' &= \left(\sum_{n=0}^{\infty}\left(\sum_{i=0}^{n} a_i b_{n-i}\right) t^n\right)' = \sum_{n=1}^{\infty}\left(n\sum_{i=0}^{n} a_i b_{n-i}\right) t^{n-1} \\
&= \sum_{n=1}^{\infty}\left(\sum_{i=0}^{n} i a_i b_{n-i} + \sum_{i=0}^{n}(n-i) a_i b_{n-i}\right) t^{n-1} \\
&= \sum_{n=1}^{\infty}\left(\sum_{i=1}^{n} i a_i b_{n-i}\right) t^{n-1} + \sum_{n=1}^{\infty}\left(\sum_{i=0}^{n-1} a_i (n-i) b_{n-i}\right) t^{n-1} \\
&= f'(t)g(t) + f(t)g'(t).
\end{aligned}$$

また，積分 $\int_0^t \sum_{n=0}^{\infty} a_n t^n \, dt$ も形式的な項別積分

$$\int_0^t \sum_{n=0}^{\infty} a_n t^n \, dt = \sum_{n=0}^{\infty} a_n \frac{t^{n+1}}{n+1} = a_0 t + a_1 \frac{t^2}{2} + a_2 \frac{t^3}{3} + a_3 \frac{t^4}{4} + \cdots$$

で定義する．

さて，ベルヌーイ数の母関数を扱うためには，形式的べき級数環を形式的ローラン級数[18]の環にまで広げておいたほうがよい．

定義 1.11　有限個の負べき項も許した R 係数の形式的ローラン級数

$$\sum_{i=-N}^{\infty} a_i t^i \qquad (N \text{ はある整数})$$

の全体の集合を $R((t))$ で表す．

$R[[t]]$ と同様にして和，積を定義することによって，$R((t))$ は $R[[t]]$ を部分

[18] 正確には，負べき項が有限個しかないローラン級数．

整域として含む可換整域になる．また 0 でない最初の係数 a_{-N} が可逆であることが，級数 $\sum_{i=-N}^{\infty} a_i t^i$ が $R((t))$ において可逆であるための必要十分条件である．これらは命題 1.8，1.9 と同様にして証明される．特に R が体であれば $R((t))$ も体となる．さらに，形式的な微分，積分も同様に定義され，商の微分公式 $(f(t)/g(t))' = (f'(t)g(t) - f(t)g'(t))/g(t)^2$ が成り立つ．これは積の微分公式から従う．（$f(t)/g(t) = h(t)$ とおいて，$f(t) = g(t)h(t)$ を微分する．）

1.4　ベルヌーイ数の母関数

定理 1.12　B_n $(n = 0, 1, 2, \cdots)$ をベルヌーイ数とする．$\mathbf{Q}((t))$ において等式

$$\frac{te^t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}$$

が成り立つ．

両辺は実際は $\mathbf{Q}[[t]]$ に入っているが，te^t の $e^t - 1$ による商は $\mathbf{Q}((t))$ において考えるのである．

証明　等式 $(\sum_{n=0}^{\infty} B_n \frac{t^n}{n!})(e^t - 1) = te^t$ を示せばよい．求める式はこの両辺を $e^t - 1$ で割ることにより得られる．積の定義から，

$$\begin{aligned}
\left(\sum_{n=0}^{\infty} B_n \frac{t^n}{n!}\right)(e^t - 1) &= \left(\sum_{n=0}^{\infty} \frac{B_n}{n!} t^n\right)\left(\sum_{n=1}^{\infty} \frac{t^n}{n!}\right) \\
&= \sum_{n=1}^{\infty} \left(\sum_{i=0}^{n-1} \frac{B_i}{i!} \frac{1}{(n-i)!}\right) t^n \\
&= \sum_{n=1}^{\infty} \left(\sum_{i=0}^{n-1} \binom{n}{i} B_i\right) \frac{t^n}{n!}.
\end{aligned}$$

ここで，ベルヌーイ数を定義する漸化式 (1.2) より $\sum_{i=0}^{n-1} \binom{n}{i} B_i = n$ がすべての $n \geq 1$ について成り立つので，最後の式は

$$\sum_{n=1}^{\infty} \left(\sum_{i=0}^{n-1} \binom{n}{i} B_i\right) \frac{t^n}{n!} = \sum_{n=1}^{\infty} \frac{t^n}{(n-1)!} = te^t$$

となり，示すべき式を得る．　∎

注意 1.13　逆に，この母関数で B_n を定義したとすると，

$$(\sum_{n=0}^{\infty} B_n \frac{t^n}{n!})(e^t - 1) = te^t$$

が成り立つので，上の証明のように左辺を展開して右辺と比べると漸化式 (1.2) が得られる．すなわち定義 1.1 と定理 1.12 の母関数表示は同値である．

母関数を使うと 3 以上の奇数番目の B_n は 0 であることが簡単にわかる．

命題 1.14（命題 1.4 再掲）　n を 3 以上の奇数とするとき $B_n = 0$.

証明　1 次の項を取り去った $\frac{te^t}{e^t-1} - \frac{t}{2}$ が偶数次の項しかもたないことを見ればよいが，

$$\frac{te^t}{e^t - 1} - \frac{t}{2} = \frac{t(e^t - 1 + 1)}{e^t - 1} - \frac{t}{2} = \frac{t}{e^t - 1} + \frac{t}{2}$$

かつ

$$\frac{(-t)e^{-t}}{e^{-t} - 1} - \frac{(-t)}{2} = \frac{-t}{1 - e^t} + \frac{t}{2} = \frac{t}{e^t - 1} + \frac{t}{2}$$

となり $\frac{te^t}{e^t-1} - \frac{t}{2}$ は $t \to -t$ で不変，すなわち奇数次の係数はすべて 0 である．∎

偶数番目の B_n については，表を見ると 0 でなく B_2 から符号が交代している．これは後に証明されるリーマンゼータ関数 $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ の偶数点での値の公式（61 ページ (4.4) 式で $k \to 2k$ とする）

$$\zeta(2k) = \frac{(-1)^{k-1}}{2} \frac{(2\pi)^{2k}}{(2k)!} B_{2k} \qquad (k \geq 1)$$

からも見てとれることであるが，ベルヌーイ数の満たす次の漸化式（Euler[19]による [25]）から直接証明しておく．

命題 1.15　$$(2n+1)B_{2n} = -\sum_{m=1}^{n-1} \binom{2n}{2m} B_{2m} B_{2(n-m)} \qquad (n \geq 2)$$

証明　まず，先の命題により，ベルヌーイ数の母関数 $\frac{te^t}{e^t-1}$ から 1 次の項を取り去ったものが

$$\frac{te^t}{e^t - 1} - \frac{t}{2} = \sum_{n=0}^{\infty} B_{2n} \frac{t^{2n}}{(2n)!}$$

---

[19]Leonhard Euler（1707.4.15 スイス Basel 生——1783.9.18 ロシア St. Petersburg 没）

と，偶数番目のベルヌーイ数の母関数となる．左辺を $f(t)$ とおく．18 ページに述べたように通常の微分計算を行って

$$f(t) - tf'(t) = f(t)^2 - \frac{t^2}{4}$$

が成り立つことがわかる．これに $f(t) = \sum_{n=0}^{\infty} B_{2n} \frac{t^{2n}}{(2n)!}$ を代入すると

$$\sum_{n=0}^{\infty} (1-2n) B_{2n} \frac{t^{2n}}{(2n)!} = \sum_{n=0}^{\infty} \left(\sum_{m=0}^{n} \binom{2n}{2m} B_{2m} B_{2(n-m)} \right) \frac{t^{2n}}{(2n)!} - \frac{t^2}{4}.$$

この両辺の係数を比べると $n \geq 2$ について

$$(1-2n) B_{2n} = \sum_{m=0}^{n} \binom{2n}{2m} B_{2m} B_{2(n-m)}.$$

右辺の $m = 0, n$ の項から $2B_{2n}$ がでるので，それを移項して -1 倍すると命題を得る．■

系 1.16　$n \geq 1$ に対し，$(-1)^{n-1} B_{2n} > 0$.

証明　帰納法による．$n = 1$ のとき $B_2 = \frac{1}{6} > 0$ で正しい．n 未満で正しいとする．命題の式は両辺に $(-1)^{n-1}$ をかけて

$$(2n+1) \cdot (-1)^{n-1} B_{2n} = \sum_{m=1}^{n-1} \binom{2n}{2m} (-1)^{m-1} B_{2m} (-1)^{n-m-1} B_{2(n-m)}$$

と書けるが，帰納法の仮定より右辺は正の数である．したがって $(-1)^{n-1} B_{2n} > 0$ となる．■

最後に，ベルヌーイ数の別の形の母関数表示として，$\tan(x), \cot(x)$ の展開を与えておこう．

命題 1.17　三角関数 $\tan(x), \cot(x)$ の原点でのテイラー（ローラン）展開は

$$\tan(x) = \sum_{n=1}^{\infty} (-1)^{n-1} (2^{2n} - 1) 2^{2n} B_{2n} \frac{x^{2n-1}}{(2n)!},$$

$$\cot(x) = \frac{1}{x} + \sum_{n=1}^{\infty} (-1)^n 2^{2n} B_{2n} \frac{x^{2n-1}}{(2n)!}$$

となる．（右辺はそれぞれ $|x| < \frac{\pi}{2}$, $0 < |x| < \pi$ で収束している．）

証明　命題 1.15 の証明中の $f(x)$（t を x にかえた）は双曲線関数 $\coth(x) = \frac{e^x + e^{-x}}{e^x - e^{-x}}$ を用いて $f(x) = \frac{x}{2} \coth(\frac{x}{2})$ と書けるので，そこでの式

$$\frac{x}{2}\coth(\frac{x}{2}) = \sum_{n=0}^{\infty} B_{2n}\frac{x^{2n}}{(2n)!}$$

は $\coth(\frac{x}{2})$ の展開を与えているものと見なすことができる．ここで，x を $2ix$ ($i = \sqrt{-1}$) とし，両辺を x で割って，$i\coth(ix) = \cot(x)$ を使うとまず $\cot(x)$ の展開式が得られる．$\cot(x)$ の倍角公式

$$\cot(2x) = \frac{1}{2}(\cot(x) - \tan(x))$$

より

$$\tan(x) = \cot(x) - 2\cot(2x)$$

なので，$\tan(x)$ の展開式は $\cot(x)$ のそれより得られる．収束域については，それぞれの原点に一番近い特異点が $\pm\pi/2$, $\pm\pi$ であることからわかる．■

注意 1.18　$\tan(x)$ の展開における $\frac{x^{2n-1}}{(2n-1)!}$ の係数

$$T_n := (-1)^{n-1}(2^{2n} - 1)2^{2n}\frac{B_{2n}}{2n}$$

は tangent number（正接数）と呼ばれることもある数で，正の整数である．正であることは系 1.16 よりわかるが，整数であることは 98 ページ注意 7.6 で証明する．このことの別の証明，および Knuth-Buckholtz [54] による T_n を用いたベルヌーイ数の計算法の解説が [64] にある．

第 2 章

スターリング数とベルヌーイ数

この章では，ベルヌーイ数をスターリング数で書き表す公式を与える．この公式は，次章で述べるクラウゼン・フォンシュタウトの定理の証明に用いられる．また，この公式の応用として，ベルヌーイ数を計算する面白いアルゴリズムも紹介する．

まずスターリング数についてまとめておく．この章で用いるのは第 2 種のほうであるが，後に第 1 種スターリング数も必要になるので同時に紹介する[1]．

2.1 スターリング数

先に第 2 種スターリング数の定義から，それも，組み合わせ的に意味のつく場合から始める．以下の定義は Knuth [52] に従った[2]．

定義 2.1（**第 2 種スターリング数**（Stirling subset number））正整数 $n, m > 0$ に対し

$$\left\{ {n \atop m} \right\} := n \text{ 元集合を } m \text{ 個の空でない部分集合に分ける方法の数}$$

---

[1]Knuth [52] によれば，Stirling（James，1692.5 イギリス Garden 生——1770.12.5 イギリス Edinburgh 没）が先に導入したのは第 2 種のほうであるという．「第 1 種，第 2 種」という命名は Nielsen（Niels，1865.12.2 デンマーク Ørslev 生——1931.9.16 デンマーク Copenhagen 没）のガンマ関数についての本 [65, §26] がはじめらしい．

[2]記法は Knuth 以前にも用いられていたようであるが，定義は符号がついたりして違っていたらしい．Knuth は [52] の中でこの定義と記法の優位を力説している．

とする．（Knuth の提案する読み方は “n subset m”.）

たとえば 4 元集合 {1,2,3,4} を 2 個の空でない部分集合に分ける方法は

$$\{1\}\cup\{2,3,4\},\ \{2\}\cup\{1,3,4\},\ \{3\}\cup\{1,2,4\},\ \{4\}\cup\{1,2,3\},$$
$$\{1,2\}\cup\{3,4\},\ \{1,3\}\cup\{2,4\},\ \{1,4\}\cup\{2,3\}$$

の 7 通りであるから $\left\{{4 \atop 2}\right\} = 7$.

定義から $m > n$ なら $\left\{{n \atop m}\right\} = 0$ である．また，この定義のもとで，次の漸化式が成り立つ．

$$\left\{{n+1 \atop m}\right\} = \left\{{n \atop m-1}\right\} + m\left\{{n \atop m}\right\}. \tag{2.1}$$

これは 2 項係数の関係式 $\binom{n+1}{m} = \binom{n}{m} + \binom{n}{m-1}$ の組み合わせ的証明と同じ要領で示される．すなわち，$n+1$ 元集合を m 個に分ける際，ある 1 つの元に着目し，それが独立の 1 元集合をなすときは残り n 元を $m-1$ 個に分けるのが $\left\{{n \atop m-1}\right\}$ 通り，他の集合の 1 要素となるときはまず残り n 元を m 個に分けるのが $\left\{{n \atop m}\right\}$ 通り，どこに入れるかが m 通りあって合計 $m\left\{{n \atop m}\right\}$ 通りとなる．

さてそこで，今度はこの漸化式によってすべての整数 m, n に対する $\left\{{n \atop m}\right\}$ を定義する．

定義 2.2（**第 2 種スターリング数（一般の場合）**）　任意の整数 n, m に対し $\left\{{n \atop m}\right\}$ を

$$\text{初期値}\ \left\{{0 \atop 0}\right\} = 1,\ \left\{{n \atop 0}\right\} = \left\{{0 \atop m}\right\} = 0\ (n, m \neq 0),\ \text{および漸化式 (2.1)}$$

で定義する．

漸化式 (2.1) から，3 つの数 $\left\{{n+1 \atop m}\right\}, \left\{{n \atop m-1}\right\}, \left\{{n \atop m}\right\}$ のうち 2 つを決めれば残りが決まる．ただし $\left\{{n \atop m}\right\}$ の前に m がかかっているので $m = 0$ のときはこれで割ることができないが，$\left\{{n \atop 0}\right\}$ は初期値として与えてあるので問題ない．26 ページに表を与えるが，3 つの数の位置関係を考えると，与えられた初期値とこの関係式からすべての $\left\{{n \atop m}\right\}$ が決まることがわかる．

こうして定義し直した $\left\{{n \atop m}\right\}$ は，$n, m > 0$ のときには先の組み合わせ的定義に一致する．それを見るには，先の定義から直ちにわかる値 $\left\{{n \atop 1}\right\} = 1\ (n \geq 1)$, $\left\{{1 \atop m}\right\} = 0\ (m \geq 2)$ がいまの定義から定まる値と一致することを確かめればよ

い．するとそれを初期値としてあとは同じ漸化式で決まっていくので同じ数になる．そのためにまず漸化式 (2.1) で $m=1$ とおいて，

$$\left\{ {n+1 \atop 1} \right\} = \left\{ {n \atop 0} \right\} + \left\{ {n \atop 1} \right\}.$$

ここで $n=0$ とすると $\left\{ {1 \atop 1} \right\} = 1$. また $n>0$ なら $\left\{ {n \atop 0} \right\} = 0$ なので $\left\{ {n+1 \atop 1} \right\} = \left\{ {n \atop 1} \right\}$, これより $\left\{ {n \atop 1} \right\} = 1\ (n \geq 1)$ となる．また，$\left\{ {1 \atop m} \right\} = 0\ (m \geq 2)$ は (2.1) で $n=0$ とおくと直ちに示される．

注意 2.3 論理的には定義 2.2 だけでよいわけだが，それでは意味がわからないので，まず定義 2.1 から始めた．

次に第 1 種スターリング数を同じ仕方で定義していこう．

定義 2.4（**第 1 種スターリング数**(Stirling cycle number)） 正整数 $n, m > 0$ に対し

$$\left[{n \atop m} \right] := m \text{ 個のサイクルからなる } n \text{ 次置換（} n \text{ 次対称群の元）の個数}$$

とする（"n cycle m"）．

つまり n 次対称群（集合 $\{1, 2, \cdots, n\}$ 上の置換（全単射）全体）の元を互いに共通の文字のない巡回置換（サイクル）の積として書いたとき（その書き方は本質的に 1 通りである．群論の教科書，たとえば [79, 3 章 §2] を参照のこと），現れるサイクルの個数（動かない文字も 1 つのサイクルとして数える）が m となる置換の個数が $\left[{n \atop m} \right]$ である．たとえば 2 つのサイクルの積となる 4 次の置換は

$$(1)(2\,3\,4),\ (1)(2\,4\,3),\ (2)(1\,3\,4),\ (2)(1\,4\,3),$$
$$(3)(1\,2\,4),\ (3)(1\,4\,2),\ (4)(1\,2\,3),\ (4)(1\,3\,2),$$
$$(1\,2)(3\,4),\ (1\,3)(2\,4),\ (1\,4)(2\,3)$$

の 11 個で，$\left[{4 \atop 2} \right] = 11$. また $\left[{n \atop n} \right] = 1$（恒等置換），$\left[{n \atop 1} \right] = (n-1)!$（$n$ 次巡回置換の個数）である．

この第 1 種スターリング数は漸化式

$$\left[{n+1 \atop m} \right] = \left[{n \atop m-1} \right] + n\left[{n \atop m} \right] \tag{2.2}$$

を満たす．これも先と同じ要領で示すことができる．すなわち，m 個のサイク

表 2.1: $\left\{ {n \atop m} \right\}$

m ＼ n	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6
6	0	0	0	0	0	0	0	0	0	0	0	0	1
5	0	0	0	0	0	0	0	0	0	0	0	1	15
4	0	0	0	0	0	0	0	0	0	0	1	10	65
3	0	0	0	0	0	0	0	0	0	1	6	25	90
2	0	0	0	0	0	0	0	0	1	3	7	15	31
1	0	0	0	0	0	0	0	1	1	1	1	1	1
0	0	0	0	0	0	0	1	0	0	0	0	0	0
-1	0	0	0	0	0	1	0	0	0	0	0	0	0
-2	0	0	0	0	1	1	0	0	0	0	0	0	0
-3	0	0	0	1	3	2	0	0	0	0	0	0	0
-4	0	0	1	6	11	6	0	0	0	0	0	0	0
-5	0	1	10	35	50	24	0	0	0	0	0	0	0
-6	1	15	85	225	274	120	0	0	0	0	0	0	0

ルからなる $n+1$ 次置換のうち，たとえば $n+1$ が動かないものはこれが 1 つのサイクル $(n+1)$ をつくり，残り n 文字が $m-1$ 個のサイクルからなるので $\left[{n \atop m-1} \right]$ 個，$n+1$ が動くものは，1 から n までの n 次置換で m 個のサイクルからなるものの中に $n+1$ を挿入することで得られる．その際，長さ j のサイクルに 1 つ別の文字を加えて長さ $j+1$ の相異なるサイクルをつくる方法は j 通りであるので，$n+1$ の入れ方は n 通りとなり，合計 $n\left[{n \atop m} \right]$ 通り，したがって (2.2) 式の右辺が得られる．

そこで第 2 種のときと同様に，

定義 2.5（第 1 種スターリング数（一般の場合））　任意の整数 n, m に対し $\begin{bmatrix} n \\ m \end{bmatrix}$ を

$$\text{初期値}\ \begin{bmatrix} 0 \\ 0 \end{bmatrix} = 1, \begin{bmatrix} n \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ m \end{bmatrix} = 0\ (n, m \neq 0),\ \text{および漸化式 (2.2)}$$

で定義する．

こちらも同じ範囲で表をあげておく．2 つの表をよく見比べていただきたい．

表 2.2: $\begin{bmatrix} n \\ m \end{bmatrix}$

m \ n	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6
6	0	0	0	0	0	0	0	0	0	0	0	0	1
5	0	0	0	0	0	0	0	0	0	0	0	1	15
4	0	0	0	0	0	0	0	0	0	0	1	10	85
3	0	0	0	0	0	0	0	0	0	1	6	35	225
2	0	0	0	0	0	0	0	0	1	3	11	50	274
1	0	0	0	0	0	0	0	1	1	2	6	24	120
0	0	0	0	0	0	0	1	0	0	0	0	0	0
-1	0	0	0	0	0	1	0	0	0	0	0	0	0
-2	0	0	0	0	1	1	0	0	0	0	0	0	0
-3	0	0	0	1	3	1	0	0	0	0	0	0	0
-4	0	0	1	6	7	1	0	0	0	0	0	0	0
-5	0	1	10	25	15	1	0	0	0	0	0	0	0
-6	1	15	65	90	31	1	0	0	0	0	0	0	0

ある著しいことに気づかれることと思う．Knuth の言うように，このことからスターリング数は実は「1 種類」であって，2 つの漸化式 (2.1)，(2.2) も本質的に同じものであることがわかる（次の命題参照）．

それも含め，スターリング数の満たすいくつかの公式を次にあげておく．ほかにも多くの公式があるが，後で必要なもののみにとどめた．さまざまな公式についてはたとえば [29] を参照のこと．

命題 2.6

(1)
$$\begin{bmatrix} n \\ m \end{bmatrix} = \begin{Bmatrix} -m \\ -n \end{Bmatrix}.$$

(2)
$$x^n = \sum_{m=0}^{n} \begin{Bmatrix} n \\ m \end{Bmatrix} (x)_m \qquad (n \geq 0).$$

ここに $(x)_m$ は[3]

[3]Knuth は $(x)_m$ を $x^{\underline{m}}$ と書くことも提案しているがここでは採らない．

$$(x)_m = x(x-1)(x-2)\cdots(x-m+1) \quad (m>0),\ (x)_0 = 1.$$

(3)
$$(x)_n = (-1)^n \sum_{m=0}^{n} (-1)^m \begin{bmatrix} n \\ m \end{bmatrix} x^m.$$

(4)
$$\left(x\frac{d}{dx}\right)^n = \sum_{m=1}^{n} \begin{Bmatrix} n \\ m \end{Bmatrix} x^m \left(\frac{d}{dx}\right)^m \qquad (n \geq 1).$$

(5.1)
$$m, n \geq 0 \text{ に対し，} \sum_{l\geq 0} (-1)^l \begin{Bmatrix} n \\ l \end{Bmatrix} \begin{bmatrix} l \\ m \end{bmatrix} = (-1)^m \delta_{m,n}.$$

(5.2)
$$m, n \geq 0 \text{ に対し，} \sum_{l\geq 0} (-1)^l \begin{bmatrix} n \\ l \end{bmatrix} \begin{Bmatrix} l \\ m \end{Bmatrix} = (-1)^m \delta_{m,n}.$$

（$\delta_{m,n}$ はクロネッカーのデルタ，すなわち $m=n$ なら 1，$m \neq n$ なら 0 を表す．左辺の和はともに実質有限である．）

(6)
$$m, n \geq 0 \text{ に対し，} \begin{Bmatrix} n \\ m \end{Bmatrix} = \frac{(-1)^m}{m!} \sum_{l=0}^{m} (-1)^l \binom{m}{l} l^n.$$

(7)
$$\frac{(e^t-1)^m}{m!} = \sum_{n=m}^{\infty} \begin{Bmatrix} n \\ m \end{Bmatrix} \frac{t^n}{n!} \qquad (m \geq 0).$$

(8)
$$\frac{t^m}{(1-t)(1-2t)\cdots(1-mt)} = \sum_{n=m}^{\infty} \begin{Bmatrix} n \\ m \end{Bmatrix} t^n \qquad (m \geq 1).$$

(9)
$$\frac{(-\log(1-t))^m}{m!} = \sum_{n=m}^{\infty} \begin{bmatrix} n \\ m \end{bmatrix} \frac{t^n}{n!} \qquad (m \geq 0).$$

証明　(1)　$a_{n,m} = \left\{ {-m \atop -n} \right\}$ とおく．これが $\left[{n \atop m} \right]$ と同じ初期値，漸化式を満たすことを確かめればよい．初期値については直ちに等しいことがわかる．漸化式 (2.1) において m を $-n$ に，n を $-m$ にかえると

$$\left\{ \begin{matrix} -m+1 \\ -n \end{matrix} \right\} = \left\{ \begin{matrix} -m \\ -n-1 \end{matrix} \right\} - n \left\{ \begin{matrix} -m \\ -n \end{matrix} \right\}.$$

移項して

$$\left\{ \begin{matrix} -m+1 \\ -n \end{matrix} \right\} + n \left\{ \begin{matrix} -m \\ -n \end{matrix} \right\} = \left\{ \begin{matrix} -m \\ -n-1 \end{matrix} \right\}$$

となるが，これは $a_{n,m-1} + na_{n,m} = a_{n+1,m}$ と書け，漸化式 (2.2) にほかならない．

(2) 同様の方針でいく．つまり $x^n = \sum_{m=0}^{n} a_{n,m}(x)_m$ とおいて $a_{n,m}$ が $m, n \geq 0$ の範囲で $\left\{ {n \atop m} \right\}$ と同じ初期値，漸化式を満たすことを確かめる．初期値はよい（ただし $a_{0,m} = 0\,(m > 0)$ とおく）．$(x)_{m+1} = (x)_m(x-m)$ より $(x)_m \cdot x = (x)_{m+1} + m(x)_m$ に注意すると，

$$\begin{aligned} \sum_{m=0}^{n+1} a_{n+1,m}(x)_m = x^{n+1} = x^n \cdot x \\ &= \sum_{m=0}^{n} a_{n,m}(x)_m \cdot x \\ &= \sum_{m=0}^{n} a_{n,m}((x)_{m+1} + m(x)_m) \\ &= \sum_{m=1}^{n+1} a_{n,m-1}(x)_m + \sum_{m=0}^{n} ma_{n,m}(x)_m. \end{aligned}$$

両辺の $(x)_m$ の係数を比べれば漸化式 (2.1) を得る．（$a_{n,-1} = a_{n,n+1} = 0$ としている．）

(3) も同様であるので省略する．

(4) は帰納法で証明する．$n = 1$ のときは両辺 $x\frac{d}{dx}$ となって等しい．n まで正しいとする．このとき

$$\begin{aligned}\left(x\frac{d}{dx}\right)^{n+1} &= \left(x\frac{d}{dx}\right)\sum_{m=1}^{n}\left\{ {n \atop m} \right\}x^m\left(\frac{d}{dx}\right)^m \\ &= x\sum_{m=1}^{n}\left\{ {n \atop m} \right\}\left(mx^{m-1}\left(\frac{d}{dx}\right)^m + x^m\left(\frac{d}{dx}\right)^{m+1}\right) \\ &= \sum_{m=1}^{n}m\left\{ {n \atop m} \right\}x^m\left(\frac{d}{dx}\right)^m + \sum_{m=1}^{n}\left\{ {n \atop m} \right\}x^{m+1}\left(\frac{d}{dx}\right)^{m+1} \\ &= \sum_{m=1}^{n+1}\left(m\left\{ {n \atop m} \right\} + \left\{ {n \atop m-1} \right\}\right)x^m\left(\frac{d}{dx}\right)^m \\ &= \sum_{m=1}^{n+1}\left\{ {n+1 \atop m} \right\}x^m\left(\frac{d}{dx}\right)^m.\end{aligned}$$

（最後から 2 つ目の等号で $\left\{ {n \atop n+1} \right\} = 0$ および $\left\{ {n \atop 0} \right\} = 0$ を用いた.）したがって $n+1$ でも正しい.

(5) は (2), (3) を使う. たとえば (5.1) は, (2) で m を l にかえた式

$$x^n = \sum_{l=0}^{n}\left\{ {n \atop l} \right\}(x)_l$$

において, (3) の n を l とした

$$(x)_l = (-1)^l\sum_{m=0}^{l}(-1)^m\left[{l \atop m} \right]x^m$$

を代入すると

$$\begin{aligned}x^n &= \sum_{l=0}^{n}\left\{ {n \atop l} \right\}(-1)^l\sum_{m=0}^{l}(-1)^m\left[{l \atop m} \right]x^m \\ &= \sum_{m=0}^{n}(-1)^m\sum_{l=m}^{n}(-1)^l\left\{ {n \atop l} \right\}\left[{l \atop m} \right]x^m.\end{aligned}$$

この両辺の係数を比べればよい. (5.2) は逆に (2) を (3) に代入して同様にする.

(6) も右辺が $\left\{ {n \atop m} \right\}$ の漸化式を満たすことを見る. 右辺をやはり $a_{n,m}$ とおこう. $a_{0,0} = 1$ および $n \geq 1$ のとき $a_{n,0} = 0$ なることはよい（$0^0 = 1$ とする）. $n = 0$ で $m \geq 1$ のとき $\sum_{l=0}^{m}(-1)^l\binom{m}{l} = (1-1)^m = 0$ より $a_{0,m} = 0$. 次に漸化式であるが,

$$
\begin{aligned}
&ma_{n,m} + a_{n,m-1} \\
&= \frac{(-1)^m}{(m-1)!}\sum_{l=0}^{m}(-1)^l\binom{m}{l}l^n + \frac{(-1)^{m-1}}{(m-1)!}\sum_{l=0}^{m-1}(-1)^l\binom{m-1}{l}l^n \\
&= \frac{(-1)^m}{(m-1)!}\sum_{l=0}^{m}(-1)^l\left\{\binom{m}{l} - \binom{m-1}{l}\right\}l^n \\
&= \frac{(-1)^m}{(m-1)!}\sum_{l=0}^{m}(-1)^l\frac{l}{m}\binom{m}{l}l^n \\
&= \frac{(-1)^m}{m!}\sum_{l=0}^{m}(-1)^l\binom{m}{l}l^{n+1} \\
&= a_{n+1,m}
\end{aligned}
$$

より成り立つ．この (6) は，「差分法におけるテイラー展開」という道具を用意しておくとより自然に導き出すこともできるが，それはたとえば [47, §58] を参照．

(7) は，まず右辺が $n = 0$ からの和とも書けることに注意（$n < m$ なら $\left\{ {n \atop m} \right\} = 0$ だから）して，右辺に (6) を代入，変形していく．

$$
\begin{aligned}
\text{右辺} &= \sum_{n=0}^{\infty}\left\{\frac{(-1)^m}{m!}\sum_{l=0}^{m}(-1)^l\binom{m}{l}l^n\right\}\frac{t^n}{n!} \\
&= \frac{(-1)^m}{m!}\sum_{l=0}^{m}(-1)^l\binom{m}{l}\left(\sum_{n=0}^{\infty}\frac{(lt)^n}{n!}\right) \\
&= \frac{(-1)^m}{m!}\sum_{l=0}^{m}(-1)^l\binom{m}{l}e^{lt} \\
&= \frac{(-1)^m}{m!}(1-e^t)^m \\
&= \frac{(e^t-1)^m}{m!} \\
&= \text{左辺}.
\end{aligned}
$$

または $(e^t - 1)^m/m! = \sum_{n=m}^{\infty} a_{n,m}\frac{t^n}{n!}$ と書いて，$a_{n,m}$ が $\left\{ {n \atop m} \right\}$ と同じ漸化式を満たすことを導いてもよい．

(8) 右辺を f_m とおく．$\left\{ {n \atop m} \right\}$ の漸化式 (2.1) より ($n < m$ なら $\left\{ {n \atop m} \right\} = 0$ に注意)

$$\begin{aligned} f_m &= \sum_{n=m}^{\infty} \left\{ n \atop m \right\} t^n \\ &= \sum_{n=m}^{\infty} \left(\left\{ n-1 \atop m-1 \right\} + m \left\{ n-1 \atop m \right\} \right) t^n \\ &= t \sum_{n=m-1}^{\infty} \left\{ n \atop m-1 \right\} t^n + mt \sum_{n=m}^{\infty} \left\{ n \atop m \right\} t^n \\ &= t f_{m-1} + mt f_m. \end{aligned}$$

よって $f_m = \frac{t}{1-mt} f_{m-1}$．また $\left\{ n \atop 1 \right\} = 1\ (n \geq 1)$ より $f_1 = \frac{t}{1-t}$，これから f_m が (8) の左辺に等しいことがわかる．

(9)　$(-\log(1-t))^m/m! = \sum_{n=m}^{\infty} a_{n,m} \frac{t^n}{n!}$ とおいて，両辺を微分すると

$$\frac{(-\log(1-t))^{m-1}}{(m-1)!} \cdot \frac{1}{1-t} = \sum_{n=m}^{\infty} a_{n,m} \frac{t^{n-1}}{(n-1)!}.$$

これより，

$$\sum_{n=m-1}^{\infty} a_{n,m-1} \frac{t^n}{n!} = (1-t) \sum_{n=m}^{\infty} a_{n,m} \frac{t^{n-1}}{(n-1)!}$$

を得，$a_{n,m}$ が $\left[n \atop m \right]$ と同じ漸化式を満たすことが確かめられる．同じ初期値をもつことも容易である．　∎

注意 2.7　スターリング数をこの命題の (2)，(3) で定義することもある．

ここでこの命題の (5.1)，(7) を用いて，前章で証明しなかった式（15 ページ）

$$\log(1+(e^t-1)) = t$$

の証明を与えておこう．これだけ証明すれば，逆の

$$e^{\log(1+t)} - 1 = t$$

は命題 1.10 より従う．（あるいは命題の (9) を用いて同様に証明してもよい.）

$$
\begin{aligned}
\log(1+(e^t-1)) &= \sum_{m=1}^{\infty}(-1)^{m-1}\frac{(e^t-1)^m}{m} \\
&= \sum_{m=1}^{\infty}(-1)^{m-1}(m-1)!\sum_{n=0}^{\infty}\left\{{n \atop m}\right\}\frac{t^n}{n!} \\
&= \sum_{n=0}^{\infty}\left(\sum_{m=1}^{\infty}(-1)^{m-1}\left[{m \atop 1}\right]\left\{{n \atop m}\right\}\right)\frac{t^n}{n!} \qquad \left((m-1)! = \left[{m \atop 1}\right]\right) \\
&= \sum_{n=0}^{\infty}(-1)^{n-1}\delta_{1,n}\frac{t^n}{n!} \\
&= t.
\end{aligned}
$$

2.2 ベルヌーイ数のスターリング数による公式

ベルヌーイ数を第 2 種スターリング数を使った有限和で書く公式が少なくとも Kronecker[4][55] 以来知られている（なお 3.2 節の von Staudt に関する記述も参照）．スターリング数は命題 2.6 (6) より 2 項係数のみの入った和で書けるから，ベルヌーイ数は「初等的な」(2 項係数と単純な整式くらいしか含まない，というほどの意味) 2 重和で書けることになる．Gould [28] は類似の公式についていろいろな考証を行っていて，ベルヌーイ数の閉じた有限の（無限和や積分を含まない）公式があること自体，(少なくとも 1970 年頃までは) あまり広く知られていなかったことを明らかにしている．彼は 1 つ予想を立てていて，それは，ベルヌーイ数を上述の意味で「初等的な」1 重の和で書く公式はないだろう，というものである．われわれの知る限り，そのような公式はこれまでのところ存在しないようである．

次の公式を証明する．

定理 2.8 $$B_n = (-1)^n\sum_{m=0}^{n}\frac{(-1)^m m!\left\{{n \atop m}\right\}}{m+1} \qquad (n \geq 0).$$

---

[4]Leopold Kronecker（1823.12.7 プロイセン Liegnitz（現ポーランド Legnica）生——1891.12.29 ドイツ Berlin 没）

証明　B_n の母関数を

$$\frac{te^t}{e^t-1}=\frac{t}{1-e^{-t}}=\frac{-\log\left(1-(1-e^{-t})\right)}{1-e^{-t}}$$

と見て，$-\log(1-t)=\sum_{m=1}^{\infty}\frac{t^m}{m}$ の t に $1-e^{-t}$ $(=t+\cdots)$ を代入して変形すると，

$$\begin{aligned}\sum_{n=0}^{\infty}B_n\frac{t^n}{n!}&=\frac{-\log\left(1-(1-e^{-t})\right)}{1-e^{-t}}\\&=\sum_{m=1}^{\infty}\frac{(1-e^{-t})^{m-1}}{m}\\&=\sum_{m=0}^{\infty}\frac{(-1)^m(e^{-t}-1)^m}{m+1}\\&=\sum_{m=0}^{\infty}\frac{(-1)^m m!}{m+1}\sum_{n=m}^{\infty}\left\{{n \atop m}\right\}\frac{(-t)^n}{n!}\qquad\text{(命題 2.6 (7))}\\&=\sum_{n=0}^{\infty}(-1)^n\left(\sum_{m=0}^{n}\frac{(-1)^m m!\left\{{n \atop m}\right\}}{m+1}\right)\frac{t^n}{n!}.\end{aligned}$$

両辺の $\dfrac{t^n}{n!}$ の係数を比べれば求める公式が得られる．∎

注意 2.9　命題 2.6 (6) を用いると

$$B_n=(-1)^n\sum_{m=0}^{n}\frac{1}{m+1}\sum_{l=0}^{m}(-1)^l\binom{m}{l}l^n$$

とも書ける．

命題 2.10（**定理 2.8 のバリエーション**）

$$B_n=\sum_{m=0}^{n}\frac{(-1)^m m!\left\{{n+1 \atop m+1}\right\}}{m+1}\qquad(n\geq 0).$$

証明　右辺の母関数を計算してもよいが，定理 2.8 を使って直接計算しよう．スターリング数の漸化式 (2.1) より

$$\left\{{n+1 \atop m+1}\right\}=\left\{{n \atop m}\right\}+(m+1)\left\{{n \atop m+1}\right\}$$

であるので，

$$\text{右辺} = \sum_{m=0}^{n} \frac{(-1)^m m! \left(\left\{ {n \atop m} \right\} + (m+1) \left\{ {n \atop m+1} \right\} \right)}{m+1}.$$

ところで $\left[{m+1 \atop 1} \right] = m!$ であるので，命題 2.6 (5.1) を使うと

$$\sum_{m=0}^{n} \frac{(-1)^m m! (m+1) \left\{ {n \atop m+1} \right\}}{m+1} = \sum_{m=0}^{n} (-1)^m \begin{bmatrix} m+1 \\ 1 \end{bmatrix} \begin{Bmatrix} n \\ m+1 \end{Bmatrix} = \delta_{1,n}.$$

したがって命題の右辺は

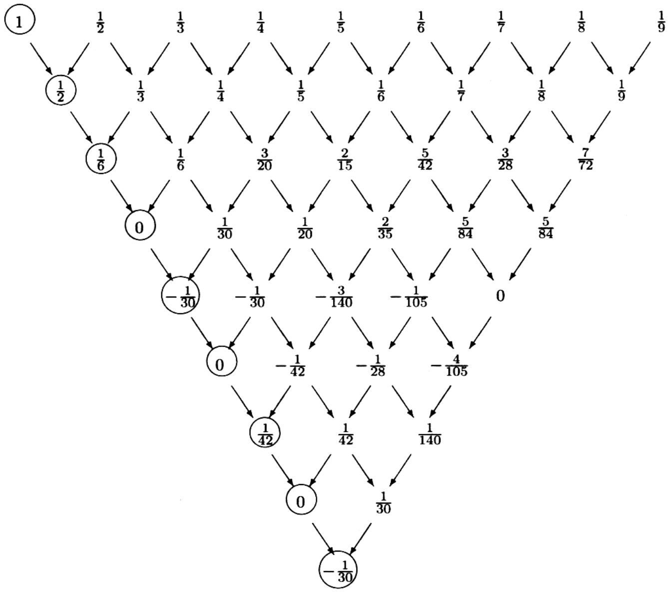
$$\sum_{m=0}^{n} \frac{(-1)^m m! \left\{ {n \atop m} \right\}}{m+1} + \delta_{1,n} = (-1)^n B_n + \delta_{1,n}$$

に等しい（定理 2.8）. $n=1$ のときこれは $-B_1 + 1 = \frac{1}{2} = B_1$，また $n \neq 1$ のときは $(-1)^n B_n$ となるが，これも B_n に等しい（9 ページ命題 1.4）. ∎

この命題は次のようなアルゴリズムとして解釈することができる[5].

まず第 0 行目（後の便宜上 1 行目ではなく 0 行目から始めることにする．以下の n 番目というのも 0 番目から始めるとする.） $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \cdots$ から出発し，第 1 行目を $1 \cdot (1 - \frac{1}{2}), 2 \cdot (\frac{1}{2} - \frac{1}{3}), 3 \cdot (\frac{1}{3} - \frac{1}{4}), \cdots$ とする．一般に，第 n 行の m 番目を $a_{n,m}$ とするとき，第 $n+1$ 行の m 番目 $a_{n+1,m}$ を $(m+1) \cdot (a_{n,m} - a_{n,m+1})$ で決める．つまり，隣どうしの差をとり，（何番目になるかの番号 +1）をかけたものを次の行に並べるのである．このとき，各行の先頭に現れる $1, \frac{1}{2}, \frac{1}{6}, 0, -\frac{1}{30}, \cdots$ がベルヌーイ数にほかならないというものである．

[5] このアルゴリズムは，多重ゼータ関数の非正整数点での値に関する秋山茂樹・谷川好男の研究 [1] において現れたものである



命題 2.10 によれば，これの証明には次がいえればよい．

命題 2.11　$a_{0,m}$ $(m=0,1,2,\cdots)$ が与えられたとし，$a_{n,m}$ $(n \geq 1)$ を

$$a_{n,m} = (m+1)\cdot(a_{n-1,m} - a_{n-1,m+1}) \qquad (n \geq 1, m \geq 0)$$

で定める．このとき，

$$a_{n,0} = \sum_{m=0}^{n} (-1)^m m! \left\{ {n+1 \atop m+1} \right\} a_{0,m}.$$

証明　母関数を用いて証明する．

$$g_n(t) = \sum_{m=0}^{\infty} a_{n,m} t^m$$

とおく．$a_{n,m}$ の漸化式より $n \geq 1$ に対して

$$
\begin{aligned}
g_n(t) &= \sum_{m=0}^{\infty}(m+1)(a_{n-1,m}-a_{n-1,m+1})t^m \\
&= \frac{d}{dt}(\sum_{m=0}^{\infty} a_{n-1,m}t^{m+1}) - \frac{d}{dt}(\sum_{m=0}^{\infty} a_{n-1,m+1}t^{m+1}) \\
&= \frac{d}{dt}(tg_{n-1}(t)) - \frac{d}{dt}(g_{n-1}(t)-a_{n-1,0}) \\
&= g_{n-1}(t) + (t-1)\frac{d}{dt}(g_{n-1}(t)) \\
&= \frac{d}{dt}((t-1)g_{n-1}(t)).
\end{aligned}
$$

よって，$(t-1)g_n(t) = h_n(t)$ とおくと，

$$
h_n(t) = (t-1)\frac{d}{dt}(h_{n-1}(t)) \qquad (n \geq 1).
$$

これより

$$
h_n(t) = \left((t-1)\frac{d}{dt}\right)^n (h_0(t))
$$

を得る．ここで命題 2.6 (4)（で $x \to t-1$ としたもの）を使うと

$$
h_n(t) = \sum_{m=0}^{n} \left\{ {n \atop m} \right\} (t-1)^m \left(\frac{d}{dt}\right)^m h_0(t).
$$

両辺 $t=0$ とおいて

$$
\begin{aligned}
-a_{n,0} &= \sum_{m=0}^{n} \left\{ {n \atop m} \right\} (-1)^m m!(a_{0,m-1}-a_{0,m}) \\
&= \sum_{m=0}^{n-1} \left\{ {n \atop m+1} \right\} (-1)^{m+1}(m+1)!a_{0,m} - \sum_{m=0}^{n} \left\{ {n \atop m} \right\} (-1)^m m!a_{0,m} \\
&= -\sum_{m=0}^{n} (-1)^m m!a_{0,m} \left((m+1)\left\{ {n \atop m+1} \right\} + \left\{ {n \atop m} \right\}\right) \\
&= -\sum_{m=0}^{n} (-1)^m m! \left\{ {n+1 \atop m+1} \right\} a_{0,m}.
\end{aligned}
$$

これで求める式が得られた． ∎

注意 2.12　2項係数を順次決めていくパスカル[6]の三角形というのがあるが，それにも似たこの逆三角形は面白い．このアルゴリズムで計算される B_1 は $\frac{1}{2}$ で，$-\frac{1}{2}$ ではない（すなわちわれわれの採用した定義のほうに合う）ことを注意しておこう．

[6]Blaise Pascal (1623.6.19 フランス Clermont 生——1662.8.19 フランス Paris 没)

第3章

クラウゼン・フォンシュタウトの定理とクンマー合同式

3.1 クラウゼン・フォンシュタウトの定理

ベルヌーイ数の分母は完全に決定することができる．これは Clausen[1] と von Staudt[2] によるもので，より詳しく，B_n の「小数部分」が次で与えられる．この結果はベルヌーイ数の p 進的性質を調べる際に基本的なものである．さらにアイゼンシュタイン[3]級数を通して，p 進モジュラー形式の理論においても基本的な役割を果たす（[72]）．

定理 3.1 $n=1$ および各偶数 $n \geq 2$ に対し，B_n は

$$B_n = -\sum_{\substack{p:\text{素数} \\ p-1|n}} \frac{1}{p} + C_n \qquad (C_n\text{は整数})$$

の形に書ける．ここで和は $p-1$ が n を割るような素数 p をわたる．(整数 a,b に対し，記号 $a|b$ は a が b を割り切ること，$a\nmid b$ は a が b を割り切らないことを表す.)

証明 $n=1$ のときはよいので，n は 2 以上の偶数とする．前章定理 2.8 の右辺の各項 $\frac{(-1)^m m!\left\{ {n \atop m} \right\}}{m+1}$ の分子は整数であるから，B_n の分母に寄与しうるのは

---

[1] Thomas Clausen（1801.1.16 デンマーク Snogbæk 生——1885.5.23 ロシア Dorpat（現エストニア Tartu）没）

[2] Karl Georg Christian von Staudt（1798.1.24 ドイツ Rothenburg ob der Tauber 生——1867.6.1 ドイツ Erlangen 没）

[3] Ferdinand Gotthold Max Eisenstein（1823.4.16 ドイツ Berlin 生——1852.10.11 ドイツ Berlin 没）

$m+1$ の約数である．したがってまず $p>n+1$ なる素数 p が B_n の分母の素因子として現れないことは明らかである．

はじめに，$m+1$ が合成数，すなわち $m+1=ab,\ 1<a,\ b<m$ と書けているとする．もし $a \neq b$ ならば ab は $m!$ を割るから $\frac{(-1)^m m!\left\{{n \atop m}\right\}}{m+1}$ は整数．また $a=b$ のとき，$2a \leq m$ ならば a および $2a$ が $m!$ を割るので $a^2=m+1$ が $m!$ を割る．したがってこのときも $\frac{(-1)^m m!\left\{{n \atop m}\right\}}{m+1}$ は整数となる．$2a>m$ ならば $2a \geq m+1$ であって，$m+1=a^2 \geq 2a \geq m+1$ より $a^2=2a$，すなわち $a=2$ となる．このとき $m=3$ で，この項がでるのは $n \geq 3$ のときである．ところがこのとき（n は偶数）28 ページ命題 2.6 (6) より，

$$
\begin{aligned}
(-1)^m m!\left\{{n \atop m}\right\} &= \sum_{l=0}^{3}(-1)^l\binom{3}{l}l^n \\
&= 0-3+3\cdot 2^n-3^n \\
&\equiv 1-(-1)^n \equiv 0 \mod 4.
\end{aligned}
$$

（整数 a,b と自然数 n について，$n|(a-b)$ のとき a と b は n を法として合同であるといい，$a \equiv b \mod n$ と書く．$n \nmid (a-b)$ のときは $a \not\equiv b \mod n$ と書く．）よってやはり $\frac{(-1)^m m!\left\{{n \atop m}\right\}}{m+1}$ は整数．以上から，$m+1$ が合成数のときは $\frac{(-1)^m m!\left\{{n \atop m}\right\}}{m+1}$ は整数であることが示された．

次に $m+1=p$（p は素数）とする．$p-1 \leq n$ である．このとき命題 2.6 (6) より，

$$
\begin{aligned}
(-1)^m m!\left\{{n \atop m}\right\} &= \sum_{l=0}^{p-1}(-1)^l\binom{p-1}{l}l^n \\
&\equiv \sum_{l=0}^{p-1} l^n \mod p \qquad \left(\tbinom{p-1}{l} \equiv (-1)^l \mod p \text{ より} \right) \\
&\equiv \begin{cases} -1 \mod p & n \text{ が } p-1 \text{ で割れるとき}, \\ 0 \mod p & n \text{ が } p-1 \text{ で割れないとき}. \end{cases} \qquad (3.1)
\end{aligned}
$$

最後の合同式は次のようにして示される．n が $p-1$ で割れるときは，フェルマーの小定理，つまり l と p が互いに素ならば $l^{p-1} \equiv 1 \mod p$ より，$\sum_{l=0}^{p-1} l^n \equiv p-1 \equiv -1 \mod p$．また，$n$ が $p-1$ で割れないならば，まず $c^n \not\equiv 1 \bmod p$ となる c をとる（たとえば $\bmod p$ の原始根）．l が 1 から $p-1$ まで動くとき，

$cl \mod p$ も 1 から $p-1$ の類をわたるから，$\sum_{l=0}^{p-1}(cl)^n \equiv \sum_{l=0}^{p-1} l^n$. よって $(c^n-1)\sum_{l=0}^{p-1} l^n \equiv 0 \mod p$ となり，$\sum_{l=0}^{p-1} l^n \equiv 0 \mod p$ である．これより，$m+1=p$ のとき $\frac{(-1)^m m!\{{n \atop m}\}}{m+1}$ は n が $p-1$ で割れないならば整数で，n が $p-1$ で割れるならば整数ではなく，このとき上の合同式から，これに $\frac{1}{p}$ を足すと整数になることがわかる．したがって定理が示された． ∎

3.2 クラウゼンとフォンシュタウト小伝

Thomas Clausen は 1801 年 1 月 16 日デンマーク Snogbæk 生まれの天文学者，数学者[4]. 貧しい小作農家の生まれで，12 才のとき，まだ読み書きもできなかったそうであるが，Nübel の牧師 Georg Holst のもとに，家畜の世話係として預けられた．数学の愛好家で天文観測も行っていた Holst は Clausen を学校に入れてやり，卒業後 7 年にわたり古典語，数学，天文学等の手ほどきをした．また Clausen も，英語，フランス語，イタリア語を独習して数学，天文学の文献を読んだ．Holst は Altona 天文台の Schumacher[5]の古くからの知り合いで，その推薦により Clausen は 1824 年，Schumacher の助手となった．Schumacher はしばしば若い才能ある人を援助した人であるが，Clausen との良好な関係は長く続かず，1 年もたたないうちに Clausen は解雇された．そのとき Clausen は Gauss[6]を訪れとりなしを乞うている．Gauss はその突然の訪問に大層驚きながらも，Schumacher に，折角の才能が駄目になってしまわないよう，よく考えてやってほしい旨の手紙を書いている（全集 XII, p.256–258)．その手紙には，「私には（Clausen は）悪気のない自然児に見えますし，高慢なところは全然ありません」「彼が際立った才能（ausgezeichnete Talente）をもっていることについては，われわれは同意見なのですから」などと書かれている．

---

[4]以下，この節の内容は Biermann [15], Noether [67] に拠っている．

[5]Heinrich Christian Schumacher（1780.9.3 ドイツ Bramstedt 生——1850 没)．はじめ法学で学位をとったが，Gauss のもとで天文学を修め天文学者となった．Abel や Jacobi の楕円関数に関する論文が載った雑誌『天文学報告』(*Astronomische Nachrichten*) の創刊者，編集者．ついでながら，Abel が Hamburg 滞在中に Clausen と会っていることが伝記（[14]）に書かれている．

[6]Johann Carl Friedrich Gauss（1777.4.30 ドイツ Brunswick 生——1855.2.23 ドイツ Göttingen 没）

結局Schumacherの斡旋で，1828年の暮れからMünchenのJoseph von Utzschneider光学研究所に，フラウンホーファー線で有名なFraunhofer[7]の後を継いで移り，研究を続けた．ここではじめ彼は随分自由な，拘束のない研究生活を送ったようである．しかし1833年はじめに病を得，詳しくは伝わっていないが，1840年頃まで，かなり厳しい時を過ごしたようである．精神障害にも悩まされたらしい．1840年6月，ClausenはAltonaのSchumacherのもとに「ぼろぼろになって」現れた．(Münchenから，お金がないのでしばしば野宿しながら，徒歩でたどり着いたという.) その途次にもClausenはGaussを訪れており，Gaussはここでも，「抽象数学の真に目覚ましい才能」が枯れてしまうのは惜しい，何か彼にしてやれないか，とSchumacherに書き送っている．Biermann [15]は「彼（Clausen）の（そのときの）財産といえば，あり余るアイデアと論文原稿だけであった」と書いているが，前節のベルヌーイ数の分母に関する結果[20]もこのとき携えてきたもののようである．これはしかしSchumacherを通じて結果は発表されたものの，その証明については明らかにされなかった．

1842年ロシアのDorpat天文台に移り（これもSchumacherの斡旋であった)，1872年の退官までそこで勤めた．Bessel[8]から絶賛された，1770年発見の彗星の軌道決定の仕事（1842年に *Astronomische Nachrichten* に発表）によりデンマーク学術協会の賞を受けた．また1854年にはGaussの推薦でGöttingenアカデミーのメンバーに，1856年にはPetersburgアカデミーのメンバーになっている．多分野にわたり150ほどの論文を書いた．いまでも彼の名前が引かれるものに，超幾何級数についてのクラウゼンの等式[9][17]や，2重対数関数のある変種“クラウゼン関数”についての仕事[18]がある．また，円周率250桁の計算[10]や，6番目のフェルマー数 $2^{2^6}+1$ の素因数分解[11]なども行っている．

---

[7]Joseph von Fraunhofer（1787.3.6 ドイツ Straubing 生——1826.6.7 ドイツ München 没）

[8]Friedrich Wilhelm Bessel（1784.7.22 ドイツ Minden 生——1846.3.17 プロイセン Königsberg（現 ロシア Kaliningrad ）没)．天文学者．ベッセル関数で有名．

[9] ${}_2F_1(\alpha,\beta,\alpha+\beta+\frac{1}{2};x)^2 = {}_3F_2\left({2\alpha,2\beta,\alpha+\beta \atop \alpha+\beta+\frac{1}{2},2\alpha+2\beta};x\right)$

[10]248桁まで正確だった．これは1847年から1853年までの記録．円周率計算の歴史や文献は[11]に詳しい．

[11]Fermatは $2^{2^n}+1$ の形の数（これをフェルマー数という）は素数ではないかと予想した．$n \le 4$ については素数になるが，Eulerが1732年，$n=5$ のときの素因数分解を与えて素数でないことを示した．2001年4月12日の時点で，$5 \le n \le 32$ なるすべての n についてフェルマー数は素数に

$2^{2^6}+1 = 274177 \cdot 67280421310721$ で，Clausen の言うところによればこの第 2 因子は当時知られていた最大の素数であった（1855.1.1 付 Gauss 宛手紙）．彼は友人で Königsberg の天文学者 C. A. F. Peters に宛てた手紙の中で，大きい数を素因数分解する新しい方法を見つけたと言っていて，そこにはやはり当時（循環小数 $1/p$ の周期に関連して）知られていなかった $(10^{17}-1)/9 = 2071723 \cdot 5363222357$ が書かれているが，「新しい方法」はついに発表されず，どのようなものであったかはわからない．

Clausen は生涯を独身で過ごし，1885 年 5 月 23 日にロシアの Dorpat（現 エストニア Tartu）で亡くなった．

Karl Georg Christian von Staudt は 1798 年 1 月 24 日，ドイツの Rothenburg ob der Tauber で生まれた．由緒ある家系で，両親，ことに優れた母親より恵まれた教育を受けたようである．Gauss の令名に惹かれ 1818 年から 1822 年まで Göttingen で学んだ．天文学にも興味をもち（当時 Gauss が当地の天文台長も兼ねていた），早くも 1820 年には火星や小惑星パラス（Pallas）の位置計算，また翌 1821 年の彗星の軌道計算などを行っており，その正確さは師 Gauss の高い称賛を受けた（von Staudt の天文計算を「非常な熟練（ausgezeichnete Geschicklichkeit）」と評している）．1835 年に Erlangen 大学の教授になるまでは，Würzburg や Nürnberg で高校の先生をしていたが，Erlangen に勤めてからは終生をそこで過ごした．1832 年に Jeanette Drechsler と結婚し一男一女をもうけた．妻が 1848 年に亡くなったが，その後再婚することはなかった．晩年はひどい喘息に悩まされたという．

彼の主な業績はその主著 "*Geometrie der Lage*"（1847）（「位置の幾何学」，射影幾何学のことをこう呼んだ）に代表される射影幾何学にあるようで，[67] でも多くの紙数を割いて彼の幾何学の業績を紹介している．ベルヌーイ数については，実は彼は前節で紹介した定理（[86]，Clausen とは独立に発見）のほかにも多くの結果を得ていたようである．Noether[12] [67] によれば，Erlangen 大学で評議会および教授会に加わる際に提出された（当時そのような習慣があった）

ならないことが知られている（ただし完全に素因数分解されているのは $n = 11$ までである）．

[12] Max Noether（1844.9.24 ドイツ Mannheim 生——1921.12.13 ドイツ Erlangen 没）

2つの論文があり[13]，そこには前章の定理2.8の公式（33ページ）や，クンマー合同式（素数を法とする場合）までも含まれているようなのであるが，「控え目な人で，流布させることなど気にもかけなかったので」まったく知られることなく埋もれてしまったらしい．（この論文の内容については [78] を参照.）ほかに Gauss の「代数学の基本定理」の証明についての論文 [87] なども発表している．（Clausen にも同じ主題の論文 [19] がある.）

喘息の苦しみの中，亡くなる1週間前にも1つ論文を書き上げているが，1867年6月1日，息を引き取った．Noether は von Staudt の人をよく表すものとして，弔辞のくだり「数ヵ月後，数年後の成果を求めるのではなく，あるはっきりした目標に向かって生涯かけて努める覚悟の定まった，彼の粘り強さ」を紹介している．

3.3　クンマー合同式

円分体の整数論，p 進 L 関数の理論などで重要な役割を果たす次の定理の証明がこの節の目標である．素数 p に対し，分母が p と互いに素な有理数全体のなす環を $\mathbf{Z}_{(p)}$ と書く．このような環を考えることで，有理数の分子が p のべきで割れるとか，有理数の間の p のべきを法とする合同などが記述しやすくなる．環 $\mathbf{Z}_{(p)}$ の可逆元の集合 $\mathbf{Z}_{(p)}^{\times}$ は，分母，分子ともに p と互いに素な有理数の全体である．また，$\mathbf{Z}_{(p)}$ の元 x, y に対し合同式 $x \equiv y \mod p^a$ が成り立つとは，$x-y$ を既約分数として書いたときに分子が p^a で割れることをいう．

定理 3.2　p を奇素数，$a \geq 1$ を自然数，m, n を $a \leq m \leq n$ なる偶数で，$p-1$ では割れず，$n \equiv m \mod (p-1)p^{a-1}$ であるとする．このとき

$$\frac{B_n}{n}, \frac{B_m}{m} \in \mathbf{Z}_{(p)}$$

であって，

$$\frac{B_n}{n} \equiv \frac{B_m}{m} \mod p^a$$

[13] ともに同じタイトル “De numeris Bernoullianis”（ベルヌーイ数について），Erlangen, 1845.

が成り立つ．

$m \geq a$ という条件をはずすとこのままでは一般には合同式は成り立たなくなり（$a \leq 2$ のときは制限になっていないのでよい），ある補正が必要になる（189 ページ定理 11.6 参照）．それが今日クンマー合同式として知られるものであるが，Kummer[14]自身が与えたものはそれや，上のものとは形が異なる（$a=1$ のときは同じ）[57]．このように定式化がかわったのはベルヌーイ数やクンマー合同式の p 進積分による自然な解釈が発見されて以降のことであろうか．Kummer 自身の証明は初等的なものであり，その方法で，上に述べた合同式ならば導くことができるので以下でそれを行う．完全な形での合同式は第 11 章で p 進積分を用いて証明される．

まず補題を用意する．

補題 3.3 p を奇素数，$\varphi(t) \in \mathbf{Z}_{(p)}[[t]]$, $r, s \in \mathbf{Z}_{(p)}$ とし，$\varphi(t)$ に $e^{rt} - e^{st} = (r-s)t + \frac{(r^2-s^2)}{2}t^2 + \cdots$ を代入して得られる形式的べき級数を次のように展開する．

$$\varphi(e^{rt} - e^{st}) = \sum_{n=0}^{\infty} A_n \frac{t^n}{n!}.$$

このとき $A_n \in \mathbf{Z}_{(p)}$ であって，任意の $m \geq a \geq 1$ に対して合同式

$$A_{m+(p-1)p^{a-1}} \equiv A_m \mod p^a$$

が成り立つ．

証明 $\varphi(t) = \sum_{k=0}^{\infty} a_k t^k$ とする．このとき，

$$\begin{aligned}
\varphi(e^{rt} - e^{st}) &= \sum_{k=0}^{\infty} a_k (e^{rt} - e^{st})^k \\
&= \sum_{k=0}^{\infty} a_k \sum_{h=0}^{k} (-1)^h \binom{k}{h} e^{rt(k-h)} e^{sth} \\
&= \sum_{k=0}^{\infty} \sum_{h=0}^{k} (-1)^h a_k \binom{k}{h} e^{(r(k-h)+sh)t}.
\end{aligned}$$

A_m はこれを t で m 回微分して $t=0$ とおいて得られる．すなわち

---

[14]Ernst Eduard Kummer（1810.1.29 ドイツ Sorau 生——1893.5.14 ドイツ Berlin 没）

$$A_m = \sum_{k=0}^{\infty} \sum_{h=0}^{k} (-1)^h a_k \binom{k}{h} (r(k-h)+sh)^m.$$

ここで，$(e^{rt}-e^{st})^k$ は t^k の項から始まるので，$k>m$ ならば上式の h に関する和は 0 になる．したがって k に関する和は実質有限である．この式の m を $m+(p-1)p^{a-1}$ にかえたものから A_m を引いて

$$\begin{aligned} &A_{m+(p-1)p^{a-1}} - A_m \\ &= \sum_{k=0}^{\infty} \sum_{h=0}^{k} (-1)^h a_k \binom{k}{h} (r(k-h)+sh)^m ((r(k-h)+sh)^{(p-1)p^{a-1}} - 1). \end{aligned}$$

ここで，$r(k-h)+sh$ が p で割れれば $m \geq a$ より $(r(k-h)+sh)^m$ が p^a で割れる．また $r(k-h)+sh$ が p で割れなければ，$(\mathbf{Z}/p^a\mathbf{Z})^\times$ の位数が $(p-1)p^{a-1}$ であるから $(r(k-h)+sh)^{(p-1)p^{a-1}}-1$ が p^a で割れることになる．いずれにせよ右辺が p^a で割れるので，

$$A_{m+(p-1)p^{a-1}} \equiv A_m \mod p^a$$

がいえた．　■

定理 3.2 の証明　p と互いに素な自然数 $c \neq 1$ に対し，

$$\varphi(t) = \frac{1}{t} - \frac{c}{(1+t)^c - 1}$$

を考える．$c \in \mathbf{Z}_{(p)}^\times$ であるので

$$\frac{(1+t)^c - 1}{c} = t + \frac{c-1}{2}t^2 + \cdots$$

は $\mathbf{Z}_{(p)}[[t]]$ に属し，また $\mathbf{Z}_{(p)}((t))$ において可逆である（19 ページ 1.3 節の最後）．

$$\frac{c}{(1+t)^c-1} = \frac{1}{t} - \frac{c-1}{2} + \frac{c^2-1}{12}t + \cdots$$

より $\varphi(t) \in \mathbf{Z}_{(p)}[[t]]$ となる．

$$\begin{aligned} \frac{t}{e^t-1} &= \frac{te^t}{e^t-1} - t \\ &= 1 - \frac{t}{2} + \sum_{n=2}^{\infty} B_n \frac{t^n}{n!} \end{aligned}$$

であるので，

$$\begin{aligned}\varphi(e^t-1)&=\frac{1}{e^t-1}-\frac{c}{e^{ct}-1}\\&=\frac{1}{t}\left(\frac{t}{e^t-1}-\frac{ct}{e^{ct}-1}\right)\\&=-\frac{1-c}{2}+\sum_{n=2}^{\infty}\left((1-c^n)\frac{B_n}{n}\cdot\frac{t^{n-1}}{(n-1)!}\right).\end{aligned}$$

よって補題（$r=1, s=0$）より $(1-c^n)\frac{B_n}{n}\in\mathbf{Z}_{(p)}$ であって，$n\equiv m \mod (p-1)p^{a-1}$ のとき

$$(1-c^n)\frac{B_n}{n}\equiv(1-c^m)\frac{B_m}{m} \mod p^a$$

である．ここで c を，法 p での原始根（$c \mod p$ が $(\mathbf{Z}/p\mathbf{Z})^\times$ の生成元）であるようにとったとすると，n が $p-1$ で割れないときは（このとき m も $p-1$ で割れない），$1-c^n, 1-c^m\in(\mathbf{Z}/p^a\mathbf{Z})^\times$ かつ $1-c^n\equiv 1-c^m \mod p^a$ となる．したがって定理の合同式が得られる． ∎

3.4 クンマー小伝

Ernst Eduard Kummer は 1810 年 1 月 29 日，ドイツの Sorau（現在ポーランドの Zary）の生まれ[15]．父は医師で Carl Gotthelf Kummer，母の旧姓は Friderike Sophie Rothe といい，Ernst は彼らの次男であった．わずか 3 才のときに父がチフス（ナポレオンの軍隊がロシアから持ち帰ったものとか）で亡くなり，それからは母の手で育てられた Kummer は，1819 年にギムナジウムに入学，1828 年に Halle 大学に進学する．母の希望どおり，兄と同じく神学をはじめ専攻したが，すぐに数学に転向，これは数学教授 Scherk[16]の影響によるものであった．もっとも Kummer ははじめ数学を哲学の「準備学問」と考えていたようで，哲学を行うのに「人間精神および全自然を律するものとしての数学は最も優れた準備学問です」と母親への手紙に書いている．(Kummer は生涯を通じ，哲学に強い興味を持ち続けた.） 1831 年には，Scherk が提示した問題を

[15] 以下の内容は Biermann [16], Hensel [31], Lampe [58] に拠っている．

[16] Heinrich Ferdinand Scherk（1798——1885）．彼もベルヌーイ数に関する論文 [71] を書いている．

扱った論文「De cosinuum et sinuum potestatibus secundum cosinus et sinus arcuum multiplicium evolvendis」[17]によって賞を受けている．同じ年，ギムナジウム教官のための試験に合格，9月10日にこの受賞論文によって博士号を授与された．Sorauのギムナジウムで1年間実習の後，1832年から1842年まで，Liegnitz（現在ポーランドのLegnica）のギムナジウムで教鞭をとった．主に教えたのは数学と物理で，週に24時間もの授業をした．この教員時代の教え子にKroneckerやJoachimsthal[18]がいる．Kummerはのちに数学者としてのみならず，教育者としても非常な名声を得ていくことになるのであるが，彼らもまたKummerによって数学への興味をかきたてられ，研究者としての方向づけを与えられたのであった．特にKroneckerはKummerから大きな影響を受け，2人は生涯にわたって師弟という間柄を越えた友情で結ばれた．その断片をKummerの全集に収められた2人の間の書簡に見ることができる．

Kummerの研究した数学はその対象が時期によりかなりはっきりと分けられる．第1期が関数論，第2期が整数論，そして最後が主に幾何であった．ギムナジウムの教員時代の10年間がちょうど関数論研究の時期と重なる．そのうちとりわけ有名なのが超幾何級数に関する論文[56]である．この論文をJacobiに送ったことからJacobi，そしてDirichlet[19]との交流が始まる．1839年，Dirichletを通じBerlinアカデミーの会員となり，1840年，Dirichletの妻のいとこにあたるOttilie Mendelssohn[20]と結婚（彼女は1848年に亡くなり，その後Bertha Cauerと再婚することになる），1842年にはDirichlet，Jacobiの推挙によりBreslau（現在ポーランドのWroclaw）大学の正教授となった．Kummerの数学研究の第2期，黄金の整数論時代がこのころから始まり，以後約20年間続くことになる．

1855年にGaussが没し，その後継者としてDirichletがBerlinを去りGöttingenに赴く．KummerはそのDirichletの後を継いで同年Berlin大学教授となった．Kummerの去ったBreslauではJoachimsthalがあとについた．このBreslau

[17]「cosとsinのべきの，変数を何倍かにしたcosとsinによる展開について」

[18]Ferdinand Joachimsthal（1818.3.9 ドイツ Goldberg（現ポーランド Zlotoryja）生——1861.4.5 ドイツ Breslau（現ポーランド Wroclaw）没）

[19]Johann Peter Gustav Lejeune Dirichlet（1805.2.13 ドイツ Düren 生——1859.5.5 ドイツ Göttingen 没）

[20]Dirichletの妻 Rebecca Mendelssohnは作曲家 Felix Mendelssohnの妹である．

のポジションには Weierstrass[21]も応募していたのだが，いずれ Weierstrass を Berlin に呼びたいと考えた Kummer の計らいで元学生の Joachimsthal の採用となったらしい．その目論みどおり，翌 1856 年，Weierstrass は Berlin の講師に採用される．1861 年，Kummer と Weierstrass によって，ドイツで最初の純粋数学のセミナーが始められ，Dirichlet，Jacobi 亡きあとの Berlin の第 2 の隆盛期を迎えていくことになる．

Kummer の講義は明快で活気があり，多くの学生を惹きつけた．ある年 Hensel[22]の出席した整数論の講義には少なくとも 250 人もの聴講者がいたという．Kummer はまた，Berlin に来てから 1874 年まで，士官学校の数学教官の職にもついていた（この職の前任も Dirichlet であった）．多くの時間を初等的な講義とその準備に割かねばならなかったはずであるが（もう Kummer がかなりな年齢のころ，ある大臣に，いまでも講義の準備はどれも入念にします，と語ったというエピソードがある），彼にとっては教えるということが，いかなるレベルにあっても喜びなのであった．また，1857/58 年，1865/66 年に学部長，1868/69 年には Berlin 大学学長という地位についた．このような多忙の中，（しかも彼はアカデミーの役職にも長くついていた．しかし彼はこのような仕事を負担だとは全然思わず，むしろ，研究のための新しい活力が得られる気晴らしのようなものと考えていたという!）60 年すぎより，今日クンマー曲面として知られる 4 次曲面の研究を代表とする幾何の研究が始まる．（円分体の整数論についての論文も引き続き 70 年代半ばまで見られる.）

彼のもとにはその人間的な魅力を慕って多くの学生が集まった．彼もまたよく学生の面倒を見，必要とあれば経済的な援助も惜しまなかったという．Kummer が Berlin で主査を務めた学位論文の数が 39（副査が 30），学生のうち 17 人がの

[21] Karl Theodor Wilhelm Weierstrass（1815.10.31 ドイツ Ostenfelde 生――1897.2.19 ドイツ Berlin 没）

[22] Kurt Hensel（1861.12.29 プロイセン Königsberg（現ロシア Kaliningrad）生――1941.6.1 ドイツ Marburg 没）

ちに大学の教官になり，その中には Fuchs[23]，du Bois-Reymond[24]，Gordan[25]，Bachmann[26]，Schwarz[27]（義理の息子にあたる），Cantor[28], Schönflies[29]といった著名な数学者がいる．

1882 年 2 月 23 日，突然自ら辞意を表明して他の教授たちを驚かせた．その理由としてあげたのが，記憶力，また論理的抽象的議論を自由に行うに足る思考力の衰えを自覚したからだという．誰もそのような兆候は認めず引き留めようとしたが，Kummer は頑として主張をかえず，結局 1883 年退官（講義は 84 年が最後という記述もある），その後はゲーテとシェイクスピアを友とし，家族に囲まれ静かな余生を送った．Berlin で Kummer の後を継いだのは Fuchs である．Kummer が亡くなったのは退官後 10 年，1893 年の 5 月 14 日であった．

---

[23]Lazarus Immanuel Fuchs（1833.5.5 ドイツ Moschin（現ポーランド Poznan）生――1902.4.26 ドイツ Berlin 没）

[24]Paul David Gustav du Bois-Reymond（1831.12.2 ドイツ Berlin 生――1889.4.7 ドイツ Freiburg 没）

[25]Paul Albert Gordan（1837.4.27 ドイツ Breslau（現ポーランド Wroclaw）生――1912.12.21 ドイツ Erlangen 没）

[26]Paul Gustav Heinrich Bachmann（1837.6.22 ドイツ Berlin 生――1920.3.31 ドイツ Weimar 没）

[27]Karl Herman Amandus Schwarz（1843.1.25 ドイツ Hermsdorf 生――1921.11.30 ドイツ Berlin 没）

[28]Georg Ferdinand Ludwig Philipp Cantor（1845.3.3 ロシア St. Petersburg 生 ――1918.1.6 ドイツ Halle 没）

[29]Arthur Moritz Schönflies（1853.4.17 ドイツ Landsberg an der Warthe（現ポーランド Gorzów）生――1928.5.27 ドイツ Frankfurt am Main 没）

第4章

一般ベルヌーイ数

この章では，ディリクレ指標について説明したのち，ベルヌーイ数を指標をつけて一般化した一般ベルヌーイ数と，変数をつけて一般化したともいえるベルヌーイ多項式を導入する．2つは互いに関連しており，以降の章のさまざまな箇所で登場する．

4.1 ディリクレ指標

ディリクレ指標と呼ばれる，整数の集合 $\mathbf{Z}$ から複素数の集合 $\mathbf{C}$ への写像を定義しよう．

定義 4.1 f を自然数とする．写像 $\chi : \mathbf{Z} \longrightarrow \mathbf{C}$ が f を法とするディリクレ指標であるとは，次の3条件を満たすときをいう．

(i) χ は乗法的，すなわち，任意の a, $b \in \mathbf{Z}$ に対し，$\chi(ab) = \chi(a)\chi(b)$.

(ii) χ の値は $\bmod f$ のみによる，すなわち，任意の $a, b \in \mathbf{Z}$ に対し，$\chi(a+bf) = \chi(a)$ である．

(iii) $(a, f) = 1$ ならば $\chi(a) \neq 0$，かつ $(a, f) \neq 1$ ならば $\chi(a) = 0$．ただし，(a, f) は a と f の最大公約数を表すとする．

特に χ_0 を，

$$\chi_0(a) = \begin{cases} 1 & (a, f) = 1, \\ 0 & (a, f) \neq 1 \end{cases}$$

で定義するとこの 3 条件を満たすが，これを（f を法とする）単位指標という．

自然数 f に対し，1 以上 f 以下の f と互いに素な整数の個数を $\varphi(f)$ で表す．$\varphi(\cdot)$ はオイラー関数と呼ばれる．a を f と互いに素な整数とするとき

$$a^{\varphi(f)} \equiv 1 \bmod f$$

が成り立つ．これは初等整数論でオイラーの定理として知られているものである．証明はたとえば高木[1][80, §10] を参照．

法 f のディリクレ指標 χ について，次が成り立つ．

補題 4.2

（1）　$a \equiv 1 \bmod f$ ならば，$\chi(a) = 1$ である．

（2）　$(a, f) = 1$ ならば，$\chi(a)^{\varphi(f)} = 1$ である．

（3）
$$\sum_{a \bmod f} \chi(a) = \begin{cases} \varphi(f) & \chi = \chi_0 \text{（単位指標）のとき，} \\ 0 & \chi \neq \chi_0 \text{ のとき．} \end{cases}$$

　左辺の a は f を法とする代表系を動く．

証明　(1)　条件 (i) で $b = 1$ として $\chi(a) = \chi(a)\chi(1)$．ここで $(a, f) = 1$ となるよう a をとると条件 (iii) から $\chi(a) \neq 0$ なので，$\chi(1) = 1$．すると条件 (ii) により $a \equiv 1 \mod f$ ならば $\chi(a) = 1$ である．

(2)　$(a, f) = 1$ とする．上記のオイラーの定理より，$a^{\varphi(f)} \equiv 1 \bmod f$ となり，

$$\chi(a)^{\varphi(f)} = \chi(a^{\varphi(f)}) = \chi(1) = 1.$$

(3)　χ が単位指標のときは $(a, f) = 1$ となる a の mod f での個数が $\varphi(f)$ であるからよい．χ が単位指標でないとき，$\chi(b) \neq 0, 1$ となる b が存在する．いま $S = \sum_{a \bmod f} \chi(a)$ とおくとき，$\chi(b)S = \sum_{a \bmod f} \chi(b)\chi(a) = \sum_{a \bmod f} \chi(ba)$ であるが，$(b, f) = 1$ であるので，a が mod f の代表系を動くとき，ba もやはり mod f の代表系を動く．したがって右辺は S に等しい．よって $(1 - \chi(b))S = 0$．$1 - \chi(b) \neq 0$ より，$S = 0$ である．　∎

ディリクレ指標は，条件より自然に乗法群 $(\mathbf{Z}/f\mathbf{Z})^\times$ の指標を与えることを注意しておく．

いま，$f' \mid f$ とし χ' は f' を法とするディリクレ指標とする．$(a, f) = 1$ ならば

---

[1] 高木貞治（1875.4.21 岐阜生——1960.2.29 東京没）

$$\chi(a) = \chi'(a)$$

となるとき，χ は $\bmod f'$ で定義されるという．f を法とするディリクレ指標 χ に対し，χ が定義される最小の f' を f_χ と書き，χ の導手と呼ぶ．定義から f_χ は f の約数である．

定義 4.3（**原始的指標**）f を法とする指標 χ が原始的とは $f = f_\chi$ のときをいう．

χ を f を法とするディリクレ指標とする．$\chi(-1)^2 = \chi((-1)^2) = \chi(1) = 1$ であるから $\chi(-1) = \pm 1$ である．

χ が偶指標であるとは $\chi(-1) = 1$ のときをいい，奇指標であるとは $\chi(-1) = -1$ のときをいう．また，χ と共役な指標 $\overline{\chi}$ を

$$\overline{\chi}(a) = \overline{\chi(a)} \qquad (\chi(a) \text{ の複素共役})$$

で定義する．$f_\chi = f_{\overline{\chi}}$ である．

例 4.4　$\chi_j : \mathbf{Z} \longrightarrow \mathbf{C}$ $(j = 0, 1, 2, 3)$ を次で定義する．

$(a, 2) \neq 1$ (すなわち $2|a$) のときは $\chi_j(a) = 0$ $(j = 0, 1, 2, 3)$.

$a \equiv 1 \bmod 8$ のときは $\chi_j(a) = 1$ $(j = 0, 1, 2, 3)$.

$a \equiv 3 \bmod 8$ のときは

$$\chi_0(a) = 1, \quad \chi_1(a) = 1, \quad \chi_2(a) = -1, \quad \chi_3(a) = -1,$$

$a \equiv 5 \bmod 8$ のときは

$$\chi_0(a) = 1, \quad \chi_1(a) = -1, \quad \chi_2(a) = -1, \quad \chi_3(a) = 1,$$

$a \equiv 7 \bmod 8$ のときは

$$\chi_0(a) = 1, \quad \chi_1(a) = -1, \quad \chi_2(a) = 1, \quad \chi_3(a) = -1$$

とする．このとき χ_j $(j = 0, 1, 2, 3)$ が 8 を法とするディリクレ指標のすべてである．χ_0 は単位指標で $f_{\chi_0} = 1$. χ_1, χ_2 は原始的指標であるが χ_3 $(= \chi_1\chi_2)$ は原始的でなく，$f_{\chi_3} = 4$ である．

4.2　一般ベルヌーイ数

法 f で定義された指標 χ に対して，一般ベルヌーイ数 $B_{n,\chi}$ は，母関数を用いて

$$\sum_{a=1}^{f} \frac{\chi(a)te^{at}}{e^{ft}-1} = \sum_{n=0}^{\infty} B_{n,\chi} \frac{t^n}{n!}$$

で定義される．以下特に断らない限り $f > 1$ かつ χ は単位指標ではないと仮定する．

$$\frac{te^{at}}{e^{ft}-1} = \frac{1}{f} + \left(\frac{a}{f} - \frac{1}{2}\right)t$$
$$+ \left(\frac{a^2}{f} - a + \frac{f}{6}\right)\frac{t^2}{2} + \left(\frac{a^3}{f} - \frac{3a^2}{2} + \frac{af}{2}\right)\frac{t^3}{6} + \cdots$$

と展開されるので，補題 4.2 (3) より，

$$B_{0,\chi} = 0,$$
$$B_{1,\chi} = \frac{1}{f}\sum_{a=1}^{f}\chi(a)a,$$
$$B_{2,\chi} = \frac{1}{f}\sum_{a=1}^{f}\chi(a)a^2 - \sum_{a=1}^{f}\chi(a)a,$$
$$B_{3,\chi} = \frac{1}{f}\sum_{a=1}^{f}\chi(a)a^3 - \frac{3}{2}\sum_{a=1}^{f}\chi(a)a^2 + \frac{f}{2}\sum_{a=1}^{f}\chi(a)a$$

などとなる．

一般には次節で定義するベルヌーイ多項式 $B_n(x)$ を用いて

$$B_{n,\chi} = f^{n-1}\sum_{a=1}^{f}\chi(a)B_n(a/f) \tag{4.1}$$

と表される（次節注意 4.10 (2)）．

ベルヌーイ数は 3 以上の奇数番目が 0 であったが，一般ベルヌーイ数では次のようになる．

命題 4.5　χ は単位指標ではないとする．$(-1)^{n-1} = \chi(-1)$ を満たす n について $B_{n,\chi} = 0$ である．すなわち，χ が偶指標ならば奇数番目，奇指標ならば偶数番目の $B_{n,\chi}$ は 0 である．

証明　母関数は

$$\sum_{a=1}^{f-1} \frac{\chi(a)te^{at}}{e^{ft}-1} = \sum_{a=1}^{f-1} \frac{\chi(f-a)te^{(f-a)t}}{e^{ft}-1}$$
$$= \chi(-1)\sum_{a=1}^{f-1} \frac{\chi(a)te^{-at}}{1-e^{-ft}}$$
$$= \chi(-1)\sum_{a=1}^{f-1} \frac{\chi(a)(-t)e^{a(-t)}}{e^{f(-t)}-1}$$

より，$\chi(-1)=1$ ならば偶関数，$\chi(-1)=-1$ ならば奇関数となる． ∎

注意 4.6 $(-1)^n=\chi(-1)$ を満たす n については必ず $B_{n,\chi}\neq 0$ である．このことは，148 ページ定理 9.6 の公式（そこでの χ を $\overline{\chi}$ とする）を通じて，$n>1$ ならば L 関数がオイラー積をもつことより $L(n,\overline{\chi})\neq 0$ となり，従う．$B_{1,\chi}\neq 0$, つまり $L(1,\overline{\chi})\neq 0$ という事実は，ディリクレの算術級数定理とほぼ等価な命題であって，Dirichlet はこれを類数公式により証明した．Dirichlet [22] や Serre [73, 第 6 章] を参照.

4.3 ベルヌーイ多項式

ベルヌーイ多項式も母関数を用いて定義されることが多いが，ここでは少し異なる方法[2]で定義してみよう．母関数表示は命題 4.9 の (5) で与えられる．

まず有理数体上の多項式環 $\mathbf{Q}[x]$ から自分自身への $\mathbf{Q}$-線形写像 $I:\ \mathbf{Q}[x]\to\mathbf{Q}[x]$ を

$$I(f)=\int_x^{x+1} f(y)\,dy \qquad (f(x)\in\mathbf{Q}[x])$$

で定義する（積分の差分）.

$$I(x^n)=\frac{1}{n+1}\left((x+1)^{n+1}-x^{n+1}\right)=x^n+(\text{低次の項})$$

であるので，I を $\mathbf{Q}[x]$ の基底 $1,x,x^2,x^3,\cdots$ で表現すると対角成分が 1 の上三角行列になる．特に I は可逆である．そこで，次のようにベルヌーイ多項式を

[2] Don Zagier 氏の教示による．

定義する．

定義 4.7　ベルヌーイ多項式 $B_n(x)$ $(n=0,1,2,\cdots)$ を

$$B_n(x) := I^{-1}(x^n)$$

で定義する．

すなわち $B_n(x)$ は $\int_x^{x+1} B_n(y)\,dy = x^n$ を満たす唯一の多項式である．I について上に述べたことより，$B_n(x)$ は最高次係数が 1（モニックという）の $\mathbf{Q}$ 係数 n 次多項式である．

例 4.8

$$B_0(x) = 1,$$

$$B_1(x) = x - \frac{1}{2},$$

$$B_2(x) = x^2 - x + \frac{1}{6},$$

$$B_3(x) = x^3 - \frac{3}{2}x^2 + \frac{1}{2}x.$$

命題 4.9

（1）　$B_n(1) = B_n$ $(n \geq 0)$．また，$n \neq 1$ ならば $B_n(0) = B_n(1) = B_n$．

（2）　$B_n(x+1) - B_n(x) = nx^{n-1}$ 　　$(n \geq 0)$．

（3）　$B'_n(x) = nB_{n-1}(x)$ 　　$(n \geq 1)$．

（4）　$B_n(1-x) = (-1)^n B_n(x)$ 　　$(n \geq 0)$．

（5）（母関数）

$$\sum_{n=0}^{\infty} B_n(x)\frac{t^n}{n!} = \frac{te^{xt}}{e^t - 1}. \tag{4.2}$$

（6）（ベルヌーイ数による具体的表示）

$$B_n(x) = \sum_{j=0}^{n} (-1)^j \binom{n}{j} B_j x^{n-j}.$$

（7）

$$\sum_{i=0}^{k-1} B_n\left(x + \frac{i}{k}\right) = k^{1-n} B_n(kx) \qquad (k \geq 1).$$

証明　(1) の前半は (5)（もちろん (1) を使わず証明する）において $x=1$ とおき，ベルヌーイ数の母関数表示（19 ページ定理 1.12）を用いる．後半は，(2) で $x=0$ とすると $n \neq 1$ のとき $B_n(1) = B_n(0)$ がでるから，前半より従う．

(2) は，定義関係式 $\int_x^{x+1} B_n(y)\,dy = x^n$ を x について微分すればよい．

(3) は，(2) より，

$$\int_x^{x+1} \frac{B_n'(y)}{n}\,dy = \frac{1}{n}\left(B_n(x+1) - B_n(x)\right) = x^{n-1}$$

であるので，定義より

$$\frac{B_n'(x)}{n} = B_{n-1}(x), \qquad \text{すなわち} \qquad B_n'(x) = nB_{n-1}(x)$$

である．

(4) も，

$$\int_x^{x+1} B_n(1-y)\,dy = -\int_{1-x}^{-x} B_n(y)\,dy = \int_{-x}^{1-x} B_n(y)\,dy$$
$$= (-x)^n = (-1)^n x^n$$

となるので，やはり定義より $(-1)^n B_n(1-x) = B_n(x)$ である．

(5) t のべき級数としての左辺に，各係数に項別に I を施したものを考えると $\sum_{n=0} x^n \frac{t^n}{n!} = e^{xt}$ となる．一方，右辺を t のべき級数と見て同様に I を施すことを考えると，線形性より $I(\frac{te^{xt}}{e^t-1}) = \frac{t}{e^t-1} I(e^{xt})$ となり，さらに

$$I(e^{xt}) = \int_x^{x+1} e^{yt}\,dy = \frac{e^{(x+1)t} - e^{xt}}{t} = \frac{e^t - 1}{t} e^{xt}$$

であるので，$I(\frac{te^{xt}}{e^t-1}) = e^{xt}$．$I$ の単射性から左辺と右辺は等しい．

(6) (5) の母関数表示の右辺を $\frac{t}{e^t-1} \cdot e^{xt}$ と見て積を計算する．

$$\frac{t}{e^t - 1} = \frac{(-t)e^{-t}}{e^{-t} - 1} = \sum_{n=0}^{\infty} (-1)^n B_n \frac{t^n}{n!}$$

であるので，

$$\frac{t}{e^t - 1} \cdot e^{xt} = \left(\sum_{n=0}^{\infty} (-1)^n B_n \frac{t^n}{n!}\right)\left(\sum_{n=0}^{\infty} \frac{(xt)^n}{n!}\right)$$
$$= \sum_{n=0}^{\infty} \left(\sum_{j=0}^{n} (-1)^j \binom{n}{j} B_j x^{n-j}\right) \frac{t^n}{n!}.$$

これより (6) の表示を得る．

(7) $$\int_x^{x+1}\sum_{i=0}^{k-1} B_n(\frac{y}{k}+\frac{i}{k})\,dy = \sum_{i=0}^{k-1}\int_x^{x+1} B_n(\frac{y+i}{k})\,dy$$
$$= \sum_{i=0}^{k-1}\int_{\frac{x+i}{k}}^{\frac{x+1+i}{k}} B_n(y)\,kdy \qquad (\tfrac{y+i}{k}\to y)$$
$$= k\int_{\frac{x}{k}}^{\frac{x}{k}+1} B_n(y)\,dy$$
$$= k\left(\frac{x}{k}\right)^n = k^{1-n}x^n.$$

これより

$$\sum_{i=0}^{k-1} B_n(\frac{x}{k}+\frac{i}{k}) = k^{1-n}B_n(x).$$

$x\to kx$ として求める式が得られる. ∎

注意 4.10

（1） 8ページの注意1.3で述べたように，ベルヌーイ多項式を用いてべき乗和の公式（2ページ (1.1) 式）を導くのは容易である．命題4.9の (2) で $n\to k+1$ として得られる

$$x^k = \frac{1}{k+1}\left(B_{k+1}(x+1) - B_{k+1}(x)\right)$$

で $x=1,2,\cdots,n$ として足すと

$$\sum_{i=1}^{n} i^k = \frac{1}{k+1}\left(B_{k+1}(n+1) - B_{k+1}(1)\right).$$

ここで，命題4.9の (1), (4), (6) より

$$B_{k+1}(n+1) - B_{k+1}(1) = (-1)^{k+1}B_{k+1}(-n) - B_{k+1}$$
$$= (-1)^{k+1}\sum_{j=0}^{k+1}(-1)^j\binom{k+1}{j}B_j(-n)^{k+1-j}$$
$$-B_{k+1}$$
$$= \sum_{j=0}^{k}\binom{k+1}{j}B_j n^{k+1-j}.$$

これに $\frac{1}{k+1}\binom{k+1}{j} = \binom{k}{j}\frac{1}{k+1-j}$ を用いれば公式 (1.1) を得る．

（2） 一般ベルヌーイ数をベルヌーイ多項式で表す式 (4.1) は次のように導く．母関数表示 (4.2) において $x\to a/f$, $t\to ft$ とすると

$$\frac{te^{ta}}{e^{ft}-1} = \frac{1}{f}\sum_{n=0}^{\infty} B_n(a/f)\frac{(ft)^n}{n!}$$

を得るので，

$$\sum_{n=0}^{\infty} B_{n,\chi}\frac{t^n}{n!} = \sum_{a=1}^{f}\frac{\chi(a)te^{ta}}{e^{ft}-1} = \sum_{a=1}^{f}\chi(a)\frac{1}{f}\sum_{n=0}^{\infty}B_n(a/f)\frac{(ft)^n}{n!}$$
$$= \sum_{n=0}^{\infty}\sum_{a=1}^{f}\chi(a)B_n(a/f)\frac{f^{n-1}t^n}{n!}.$$

係数を比べて

$$B_{n,\chi} = f^{n-1}\sum_{a=1}^{f}\chi(a)B_n(a/f)$$

を得る．

さらにベルヌーイ多項式に関して，1 つの美しい公式を取り上げよう．

定理 4.11　k を自然数とするとき

$$B_k(x-[x]) = -\frac{k!}{(2\pi i)^k}\sum_{\substack{n\in\mathbf{Z}\\ n\neq 0}}\frac{e^{2\pi inx}}{n^k} \tag{4.3}$$

が，$k \geq 2$ ならばすべての実数 x について，$k=1$ ならば $x \notin \mathbf{Z}$ に対して成り立つ．ここに和は n が 0 でない整数全体をわたることを意味し，$[x]$ はガウス記号，すなわち，x 以下の最大の整数を表す．ただし $k=1$ のとき右辺の無限和は

$$\lim_{N\to\infty}\sum_{\substack{n=-N\\ n\neq 0}}^{N}\frac{e^{2\pi inx}}{n}$$

と理解する．$k \geq 2$ ならば (4.3) 式の右辺は絶対かつ x について一様に収束する．

証明　$0<x<1$ とし，関数

$$f(\zeta) = \frac{e^{x\zeta}}{e^{\zeta}-1}$$

を ζ の有理型関数と考えて，部分分数展開する．$f(\zeta)$ の極は $\zeta = 2\pi in$ $(n\in\mathbf{Z})$ で，すべて 1 位の極である．$\zeta = 2\pi in$ での留数は，

$$\lim_{\zeta\to 2\pi in}(\zeta-2\pi in)f(\zeta) = \lim_{t\to 0} t\cdot\frac{e^{x(t+2\pi in)}}{e^{t+2\pi in}-1} = e^{2\pi inx}$$

で与えられる．N を十分大なる自然数とし，$R = 2\pi(N + 1/2)$ とおく．ζ 平面の4点 $R + iR$, $-R + iR$, $-R - iR$, $R - iR$ を結ぶ道を C_N と記す．t を C_N の内部にある $t \neq 2\pi in$ $(n \in \mathbf{Z})$ なる点とすると，留数定理により

$$\int_{C_N} \frac{f(\zeta)}{\zeta - t}\, d\zeta = 2\pi i \left(f(t) + \sum_{n=-N}^{N} \frac{e^{2\pi inx}}{2\pi in - t} \right)$$

$$= 2\pi i \left(f(t) - \frac{1}{t} - \sum_{\substack{n=-N \\ n \neq 0}}^{N} \frac{e^{2\pi inx}}{t - 2\pi in} \right)$$

となる．$N \to \infty$ のとき，

$$\int_{C_N} \frac{f(\zeta)}{\zeta - t}\, d\zeta \to 0$$

が示せるので，$0 < |t| < 2\pi$ とすると

$$f(t) = \frac{1}{t} + \lim_{N \to \infty} \sum_{\substack{n=-N \\ n \neq 0}}^{N} \frac{e^{2\pi inx}}{t - 2\pi in}$$

$$= \frac{1}{t} - \lim_{N \to \infty} \sum_{\substack{n=-N \\ n \neq 0}}^{N} \frac{e^{2\pi inx}}{2\pi in \left(1 - \frac{t}{2\pi in}\right)}$$

$$= \frac{1}{t} - \lim_{N \to \infty} \sum_{\substack{n=-N \\ n \neq 0}}^{N} \frac{e^{2\pi inx}}{2\pi in} \sum_{k=1}^{\infty} \left(\frac{t}{2\pi in} \right)^{k-1}.$$

$k \geq 2$ のとき，和

$$\sum_{\substack{n=-\infty \\ n \neq 0}}^{\infty} \sum_{k=2}^{\infty} \frac{e^{2\pi inx}}{(2\pi in)^k} t^{k-1}$$

は絶対収束するので，上の式は

$$f(t) = \frac{1}{t} - \lim_{N \to \infty} \sum_{\substack{n=-N \\ n \neq 0}}^{N} \frac{e^{2\pi inx}}{2\pi in} - \sum_{\substack{n=-\infty \\ n \neq 0}}^{\infty} \sum_{k=2}^{\infty} \frac{e^{2\pi inx}}{(2\pi in)^k} t^{k-1}$$

となる．ベルヌーイ多項式の母関数表示 (4.2) は各実数 x に対して t の関数

$te^{xt}/(e^t-1)$ の $t=0$ の周りでのテイラー展開を与えているものとも見なせるので

$$f(t)=\sum_{k=0}^{\infty}B_k(x)\frac{t^{k-1}}{k!}$$

である．したがって係数を比較して

$$B_1(x)=-\lim_{N\to\infty}\sum_{\substack{n=-N\\ n\neq 0}}^{N}\frac{e^{2\pi inx}}{2\pi in},$$

$$B_k(x)=-k!\sum_{\substack{n=-\infty\\ n\neq 0}}^{\infty}\frac{e^{2\pi inx}}{(2\pi in)^k}\qquad(k\geq 2)$$

が得られる．$k\geq 2$ なら右辺の級数は x について閉区間 $[0,1]$ 上で一様収束し，$B_k(x)$ もこの範囲で連続だから，$[0,1]$ でこの式は成立する．さらに右辺はともに x について周期 1 をもつので，左辺を周期的に拡張して公式 (4.3) を得る．∎

この定理から，次章でその性質を述べるリーマンゼータ関数の，正の偶数点での値が求められる．

系 4.12 k を 2 以上の偶数とする．このとき

$$\sum_{n=1}^{\infty}\frac{1}{n^k}=-\frac{1}{2}\frac{B_k}{k!}(2\pi i)^k. \tag{4.4}$$

いくつか例をあげると，

$$\sum_{n=1}^{\infty}\frac{1}{n^2}=\frac{\pi^2}{6},\quad \sum_{n=1}^{\infty}\frac{1}{n^4}=\frac{\pi^4}{90},\quad \sum_{n=1}^{\infty}\frac{1}{n^6}=\frac{\pi^6}{945},\quad \sum_{n=1}^{\infty}\frac{1}{n^8}=\frac{\pi^8}{9450},$$

など．

証明 定理で $x=0$ とおけばよい．左辺は命題 4.9 (1) より B_k に等しく，右辺の和は k が偶数だから n が正の和の 2 倍となり求める公式が得られる． ∎

注意 4.13 定理の公式は次のようにも書き換えられる．

(1) k が偶数のとき

$$B_k(x-[x])=2(-1)^{k/2-1}k!\sum_{n=1}^{\infty}\frac{\cos 2\pi nx}{(2\pi n)^k}.$$

(2) k が奇数のとき

$$B_k(x-[x]) = 2(-1)^{(k+1)/2}k!\sum_{n=1}^{\infty}\frac{\sin 2\pi nx}{(2\pi n)^k},$$

ただし，$k=1$ のときは x は整数ではないとする．

この定理 4.11 には次のような興味深い応用がある[3]．次のようなゼータ関数の特殊値を考えよう．a, b は 0 とは異なる整数とし，p, q, r は正の偶数とする．

$$S(p,q,r;a,b) = \sum_{\substack{m\neq 0,\ n\neq 0\\ am+bn\neq 0}}\frac{1}{m^p n^q (am+bn)^r}$$

とおく．ただし m, n は条件 $m\neq 0,\ n\neq 0,\ am+bn\neq 0$ を満たす整数全体を動く．

命題 4.14　p, q, r は正の偶数とする．このとき

$$\pi^{-p-q-r}S(p,q,r;a,b)\in\mathbf{Q}$$

である．

証明　$l=-(am+bn)$ とおいて l を定める．$S(p,q,r;a,b)$ を積分表示すると記法 $\mathbf{e}(w)=e^{2\pi iw}$ を用いて

$$\begin{aligned}
S(p,q,r;a,b) &= \sum_{\substack{m,\,n,\,l\in\mathbf{Z}\\ m,\,n,\,l\neq 0,\ am+bn+l=0}}\frac{1}{m^p n^q l^r}\\
&= \sum_{\substack{m,\,n,\,l\in\mathbf{Z}\\ m,\,n,\,l\neq 0}}\int_0^1\frac{\mathbf{e}((am+bn+l)x)}{m^p n^q l^r}\,dx\\
&= \int_0^1\sum_{\substack{m,\,n,\,l\in\mathbf{Z}\\ m,\,n,\,l\neq 0}}\frac{\mathbf{e}((am+bn+l)x)}{m^p n^q l^r}\,dx\\
&= \int_0^1\sum_{\substack{m\in\mathbf{Z}\\ m\neq 0}}\frac{\mathbf{e}(amx)}{m^p}\sum_{\substack{n\in\mathbf{Z}\\ n\neq 0}}\frac{\mathbf{e}(bnx)}{n^q}\sum_{\substack{l\in\mathbf{Z}\\ l\neq 0}}\frac{\mathbf{e}(lx)}{l^r}\,dx.
\end{aligned}$$

$p, q, r\geq 2$ であるので，級数 $\sum_{m\neq 0}\frac{\mathbf{e}(amx)}{m^p}$ 等は閉区間 $[0,1]$ で一様収束することを用いた．公式 (4.3) を用いると

[3] これは Don Zagier 氏が 1999 年秋に九州大学で行った講演に基づく．

$$S(p,q,r;a,b)=\frac{(-1)^{\frac{p+q+r-2}{2}}(2\pi)^{p+q+r}}{p!q!r!}\int_0^1 B_p(ax-[ax])B_q(bx-[bx])B_r(x)\,dx$$

が従い，積分の値は有理数となる（ベルヌーイ多項式は有理数係数の多項式）ので命題の主張が得られる．∎

例 4.15（$p=q=r=2,\ a=b=1$）上述の式より

$$S(2,2,2;1,1)=\frac{(2\pi)^6}{8}\int_0^1 B_2(x)^3\,dx.$$

$B_1'(x)=1, B_2'(x)=2B_1(x)$ を使って部分積分により計算すると

$$\begin{aligned}
\int_0^1 B_2(x)^3\,dx &= \int_0^1 B_1'(x)B_2(x)^3\,dx \\
&= \Big[B_1(x)B_2(x)^3\Big]_0^1-\int_0^1 6B_1(x)^2B_2(x)^2\,dx \\
&= B_2^3-2\int_0^1 \Big(B_1(x)^3\Big)'B_2(x)^2\,dx \\
&= B_2^3-2\Big[B_1(x)^3B_2(x)^2\Big]_0^1+\frac{8}{5}\int_0^1 \Big(B_1(x)^5\Big)'B_2(x)\,dx \\
&= B_2^3-\frac{1}{2}B_2^2+\frac{8}{5}\Big[B_1(x)^5B_2(x)\Big]_0^1-\frac{16}{5}\int_0^1 B_1(x)^6\,dx \\
&= B_2^3-\frac{1}{2}B_2^2+\frac{1}{10}B_2-\frac{16}{35}\Big[B_1(x)^7\Big]_0^1 \\
&= \frac{1}{2^2\cdot 3^3\cdot 5\cdot 7}
\end{aligned}$$

となり，

$$S(2,2,2;1,1)=\frac{2\pi^6}{3^3\cdot 5\cdot 7}.$$

第 5 章

オイラー・マクローリンの和公式とリーマンゼータ関数

べき乗和の公式を別にすれば，ベルヌーイ数が現れる数学のトピックとして最もポピュラーなものが Euler-Maclaurin[1]の和公式であり，リーマンゼータ関数の整数点での値であろう．この章ではこれらスタンダードな話題をひととおり解説する．

5.1 オイラー・マクローリンの和公式

以下のオイラー・マクローリンの和公式は，関数の整数点でとる値の和を評価する際に非常に有効な手段を与える．

定理 5.1 a, b を $a \leq b$ なる任意の整数とし，M を任意の自然数とする．$f(x)$ を区間 $[a,b]$ 上で M 回連続微分可能[2]な関数とするとき，

$$\sum_{n=a}^{b} f(n) = \int_a^b f(x)dx + \frac{1}{2}(f(a)+f(b)) + \sum_{k=1}^{M-1} \frac{B_{k+1}}{(k+1)!}(f^{(k)}(b) - f^{(k)}(a)) - \frac{(-1)^M}{M!}\int_a^b B_M(x-[x])f^{(M)}(x)dx$$

[1] Colin Maclaurin（1698.2 イギリス Kilmodan 生——1746.6.14 イギリス Edinburgh 没）

[2] M 回微分可能で，M 階導関数が連続であること．

が成り立つ．B_{k+1} はベルヌーイ数，$B_M(x)$ はベルヌーイ多項式であり，$M=1$ のときは右辺の和の項は 0 と見なす．

注意 5.2

（1）　$f(n)$ を底辺が区間 $[n-\frac{1}{2}, n+\frac{1}{2}]$，高さ $f(n)$ の長方形の面積と思うと，右辺第 2 項までが左辺のいわば第 1 近似であり，さらに高位の近似を区間 $[a,b]$ の両端での情報で与えているのが次の和の項であると見ることができる．

（2）　あとで証明するリーマンゼータ関数の負整数点での値 $\zeta(-k)=-\frac{B_{k+1}}{k+1}$ を用いて公式を表すと，

$$\begin{aligned}\sum_{n=a}^{b} f(n) = \int_a^b f(x)dx + \frac{1}{2}(f(a)+f(b)) \\ - \sum_{k=1}^{M-1} \frac{\zeta(-k)}{k!}(f^{(k)}(b)-f^{(k)}(a)) \\ - \frac{(-1)^M}{M!}\int_a^b B_M(x-[x])f^{(M)}(x)dx\end{aligned}$$

となる．

この公式が役立つ例をあとで示すことにして，まずは定理 5.1 を証明しよう．

証明　$g(x)$ を区間 $[0,1]$ 上の M 回連続微分可能な関数とする．まず，$B_1'(x)=1$ に注意して $(B_1(x)=x-\frac{1}{2})$，部分積分より

$$\begin{aligned}\int_0^1 g(x)dx &= [B_1(x)g(x)]_0^1 - \int_0^1 B_1(x)g'(x)\,dx \\ &= \frac{1}{2}(g(1)+g(0)) - \int_0^1 B_1(x)g'(x)\,dx.\end{aligned}$$

$B_k(x)=\frac{1}{k+1}B_{k+1}'(x)$（56 ページ命題 4.9 の (3)）を用いて部分積分を繰り返すと，

$$\begin{aligned}\int_0^1 g(x)dx &= \frac{1}{2}\left(g(1)+g(0)\right) - \frac{1}{2}\left[B_2(x)g'(x)\right]_0^1 + \frac{1}{2}\int_0^1 B_2(x)g''(x)\,dx \\ &= \frac{1}{2}\left(g(1)+g(0)\right) - \frac{1}{2}\left[B_2(x)g'(x)\right]_0^1 \\ &\quad + \frac{1}{2\cdot 3}\left[B_3(x)g''(x)\right]_0^1 - \frac{1}{2\cdot 3}\int_0^1 B_3(x)g'''(x)\,dx \\ &= \cdots\cdots \\ &= \frac{1}{2}\left(g(1)+g(0)\right) + \sum_{k=1}^{M-1}\frac{(-1)^k}{(k+1)!}\left[B_{k+1}(x)g^{(k)}(x)\right]_0^1 \\ &\quad + \frac{(-1)^M}{M!}\int_0^1 B_M(x)g^{(M)}(x)\,dx.\end{aligned}$$

ここで，$k \geq 2$ のとき $B_k(0) = B_k(1) = B_k$ であり（命題 4.9 の(1)），また $k \geq 2$ のとき $(-1)^k B_k = B_k$（9 ページ命題 1.4）であるから，

$$\begin{aligned}\int_0^1 g(x)dx = \frac{1}{2}\left(g(1)+g(0)\right) - \sum_{k=1}^{M-1}\frac{B_{k+1}}{(k+1)!}\left(g^{(k)}(1) - g^{(k)}(0)\right) \\ + \frac{(-1)^M}{M!}\int_0^1 B_M(x)g^{(M)}(x)\,dx.\end{aligned}$$

したがって

$$\begin{aligned}\frac{1}{2}\left(g(1)+g(0)\right) = \int_0^1 g(x)dx + \sum_{k=1}^{M-1}\frac{B_{k+1}}{(k+1)!}(g^{(k)}(1) - g^{(k)}(0)) \\ - \frac{(-1)^M}{M!}\int_0^1 B_M(x)g^{(M)}(x)dx.\end{aligned}$$

ここで，関数 $g(x)$ として $f(x+n)$ をとる（$a \leq n \leq b-1$）．区間 $[0,1]$ での $B_M(x)$ を周期的に拡張した $B_M(x-[x])$ を考えると任意の整数 n と $n \leq x < n+1$ に対して $B_M(x-n) = B_M(x-[x])$ となることから，

$$\frac{1}{2}(f(n+1)+f(n)) = \int_n^{n+1} f(x)dx + \sum_{k=1}^{M-1} \frac{B_{k+1}}{(k+1)!}(f^{(k)}(n+1) - f^{(k)}(n))$$
$$-\frac{(-1)^M}{M!}\int_n^{n+1} B_M(x-[x])f^{(M)}(x)dx$$

を得る．この式を $n=a$ から $n=b-1$ まで足しあわせて，両辺に $\frac{1}{2}(f(a)+f(b))$ を加えると定理の公式を得る． ∎

5.2 リーマンゼータ関数

複素変数 z に対する指数関数 e^z は

$$e^z = 1 + z + \frac{z^2}{2!} + \cdots + \frac{z^n}{n!} + \cdots$$

で定義される．右辺の無限級数は任意の $z \in \mathbf{C}$ に対し絶対収束し，z のべき級数なので全 z 平面の正則関数になる．べき級数の積の計算から，e^z に対しては複素数の範囲でも指数法則

$$e^{z+w} = e^z e^w$$

が成り立つ．特に，$x,\ y \in \mathbf{R}$ についてはオイラーの公式

$$e^{x+iy} = e^x e^{iy} = e^x(\cos y + i \sin y)$$

が成り立っている．

一般に正の実数 a の複素数べきを，$s \in \mathbf{C}$ に対して

$$a^s = e^{s \log a}$$

で定義する．この絶対値は，$\sigma = \mathrm{Re}(s)$ とおくとき，

$$|a^s| = e^{\sigma \log a}$$

で与えられる．

s を複素数とし，最初に和

$$\sum_{n=1}^{N} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \cdots + \frac{1}{N^s}$$

を考えよう．n^s はいま述べた意味での n の複素数べきである．いま，関数 $f:(0,\infty) \longrightarrow \mathbf{C}$ を

$$f(x) = x^{-s}$$

で定義する．この $f(x)$ にオイラー・マクローリンの和公式を $a=1, b=N$ として適用する．非負整数 k に対して記号 $(s)_k$ を

$$(s)_k = \begin{cases} s(s+1)\cdots(s+k-1) & k \geq 1 \text{ のとき}, \\ 0 & k = 0 \text{ のとき} \end{cases}$$

で定める[3]と，f の k 階の導関数は

$$f^{(k)}(x) = (-s)(-s-1)\cdots(-s-k+1)x^{-s-k}$$

$$= (-1)^k (s)_k \, x^{-s-k}$$

で与えられる．また $s \neq 1$ なら

$$\int_1^N x^{-s} dx = \frac{1}{s-1}\left(1 - \frac{1}{N^{s-1}}\right)$$

となるので，定理 5.1 により，$s \neq 1$ なら

$$\sum_{n=1}^{N} \frac{1}{n^s} = \frac{1}{s-1}\left(1 - \frac{1}{N^{s-1}}\right) + \frac{1}{2}\left(1 + \frac{1}{N^s}\right) + \sum_{k=1}^{M-1} \frac{B_{k+1}}{(k+1)!} \cdot (s)_k \left(1 - \frac{1}{N^{s+k}}\right) - \frac{(s)_M}{M!} \int_1^N B_M(x-[x])x^{-s-M}\, dx \quad (5.1)$$

となる（$(-1)^k B_{k+1} = -B_{k+1}$ を用いた）．また $s=1$ のときは，$\int_1^N x^{-1}\, dx = \log N$，$(1)_k = k!$ より

$$\sum_{n=1}^{N} \frac{1}{n} = \log N + \frac{1}{2}\left(1 + \frac{1}{N}\right) + \sum_{k=1}^{M-1} \frac{B_{k+1}}{k+1}\left(1 - \frac{1}{N^{1+k}}\right) - \int_1^N B_M(x-[x])x^{-1-M} dx \quad (5.2)$$

となる．これらの公式の応用として，次の初歩的な結果を得る．

---

[3] 同じ記号を，27 ページの $(x)_m$ とは違うものとして定義しているので注意．ここでの記号はこの節でしか使わない．

命題 5.3

（1）　$\mathrm{Re}(s) > 1$ ならば，級数 $\displaystyle\sum_{n=1}^{\infty} \frac{1}{n^s}$ は絶対収束する．また，級数 $\displaystyle\sum_{n=1}^{\infty} \frac{1}{n}$ は発散する．

（2）　数列 $\{a_N\}$ を $a_N = \displaystyle\sum_{n=1}^{N} \frac{1}{n} - \log N$ で定義すると，$\{a_N\}$ は収束する．極限値 $\gamma = \displaystyle\lim_{N\to\infty} a_N$ はオイラー定数[4]と呼ばれ，任意の自然数 M に対し，

$$\gamma = \sum_{k=0}^{M-1} \frac{B_{k+1}}{k+1} - \int_1^{\infty} \frac{B_M(x-[x])}{x^{M+1}}\,dx$$

と表される．特に $M = 1$ として，

$$\gamma = 1 - \int_1^{\infty} \frac{x-[x]}{x^2}\,dx.$$

証明　(1) $\mathrm{Re}(s) = \sigma$ とする．$\displaystyle\sum_{n=1}^{N} \left|\frac{1}{n^s}\right| = \sum_{n=1}^{N} \frac{1}{n^\sigma}$ であるから，公式 (5.1) において $s = \sigma$, $M = 1$ とすると，

$$\sum_{n=1}^{N} \frac{1}{n^\sigma} = \frac{1}{\sigma-1}\left(1 - \frac{1}{N^{\sigma-1}}\right) + \frac{1}{2}\left(1 + \frac{1}{N^\sigma}\right) - \sigma \int_1^N B_1(x-[x])x^{-\sigma-1}\,dx$$

となる．$\sigma > 1$ より $1/N^{\sigma-1}$, $1/N^\sigma$ はともに $N \to \infty$ のとき 0 に収束する．最後の積分であるが，関数 $B_M(x-[x])$ は $0 \le x-[x] \le 1$ より有界であるので，積分

$$\int_1^{\infty} x^{-\sigma-1}\,dx = \lim_{N\to\infty} \int_1^N x^{-\sigma-1}\,dx \tag{5.3}$$

が収束すれば，$N \to \infty$ のとき，

$$\int_1^N B_M(x-[x])x^{-\sigma-1}\,dx$$

も収束する．積分 (5.3) は $\sigma > 0$ であれば

$$\lim_{N\to\infty} \int_1^N x^{-\sigma-1}\,dx = \lim_{N\to\infty} \frac{1}{\sigma}\left(1 - \frac{1}{N^\sigma}\right) = \frac{1}{\sigma}$$

より収束する．以上より $\sigma > 1$ のとき $\displaystyle\sum_{n=1}^{\infty} \frac{1}{n^s}$ は絶対収束する．また，$\displaystyle\sum_{n=1}^{\infty} \frac{1}{n}$

---

[4] $\gamma = 0.5772156649015328606065120900824\cdots$ で，この数が無理数かどうかもわかっていない．

が発散することは (5.2) より直ちに従う.

(2) 公式 (5.2) より

$$a_N = \sum_{n=1}^{N} \frac{1}{n} - \log N = \frac{1}{2}\left(1+\frac{1}{N}\right) + \sum_{k=1}^{M-1} \frac{B_{k+1}}{k+1}\left(1-\frac{1}{N^{1+k}}\right)$$
$$- \int_1^N B_M(x-[x])x^{-1-M}dx$$

となる．(1) におけると同様に最後の積分は収束し，したがって $\{a_N\}$ は収束する．

ここで $N \to \infty$ とすると，

$$\gamma = \lim_{N\to\infty} a_N = \frac{1}{2} + \sum_{k=1}^{M-1} \frac{B_{k+1}}{k+1} - \int_1^\infty B_M(x-[x])x^{-1-M}\,dx$$
$$= \sum_{k=0}^{M-1} \frac{B_{k+1}}{k+1} - \int_1^\infty B_M(x-[x])x^{-1-M}\,dx$$

が得られる（$B_1 = 1/2$ を用いた）．$M=1$ のとき，$B_1(x-[x]) = x-[x]-\frac{1}{2}$ で，

$$\int_1^\infty \frac{dx}{x^2} = \left[-\frac{1}{x}\right]_1^\infty = 1$$

であるので，

$$\gamma = \frac{1}{2} - \int_1^\infty \frac{x-[x]-\frac{1}{2}}{x^2}\,dx$$
$$= 1 - \int_1^\infty \frac{x-[x]}{x^2}\,dx.$$

■

有名なリーマン[5]のゼータ関数 $\zeta(s)$ は $\mathrm{Re}(s)>1$ である複素数 s に対して

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

で定義される．すでに見たように右辺の無限級数は $\mathrm{Re}(s)>1$ の範囲で絶対収

[5]Georg Friedrich Bernhard Riemann（1826.9.17 ドイツ Breselenz 生——1866.7.20 イタリア Selasca 没）

束する．1より大なる正数 σ をとると，この級数は $\mathrm{Re}(s) \geq \sigma$ の範囲で一様収束するので，$\mathrm{Re}(s) > 1$ で複素関数として s の正則関数になる．ここでは和公式 (5.1) を用いて $\zeta(s)$ の性質を調べてみる．$\mathrm{Re}(s) > 1$ とし，(5.1) において，$N \to \infty$ とすると，

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \frac{1}{s-1} + \frac{1}{2} + \sum_{k=1}^{M-1} \frac{B_{k+1}}{(k+1)!} \cdot (s)_k \tag{5.4}$$

$$-\frac{(s)_M}{M!} \int_1^{\infty} B_M(x-[x]) x^{-s-M}\, dx.$$

右辺の積分は $\mathrm{Re}(s) > 1-M$ の範囲で絶対収束するので，公式 (5.4) は $\zeta(s)$ の $\mathrm{Re}(s) > 1-M$ の範囲の有理型関数への解析接続を与える．すなわち，$\zeta(s)$ は (5.4) 式を通して自然に $\mathrm{Re}(s) > 1-M$ で定義された関数に伸びている．そこで，M は任意の自然数にとれることから，$\zeta(s)$ は全 s 平面の有理型関数に解析接続され，(5.4) 式により，極は $s=1$ のみで，$s=1$ での留数は 1 であることもわかる．

ここで，(5.1) と (5.4) の差をとると，$\mathrm{Re}(s) > 1$ の範囲で，

$$\zeta(s) - \sum_{n=1}^{N} \frac{1}{n^s} = \frac{1}{s-1} \cdot \frac{1}{N^{s-1}} - \frac{1}{2N^s} + \sum_{k=1}^{M-1} \frac{B_{k+1}}{(k+1)!} \cdot (s)_k \cdot \frac{1}{N^{s+k}}$$

$$-\frac{(s)_M}{M!} \int_N^{\infty} B_M(x-[x]) x^{-s-M}\, dx \tag{5.5}$$

となる．この式は解析数論への応用上（種々の評価等）便利なようである．

ここまでの結果をまとめて，さらに $\zeta(s)$ の 0 以下の整数点における値を求めてみよう．

定理 5.4

（1）　$\zeta(s)$ は全 s 平面の有理型関数に解析接続され，$s \neq 1$ で $\zeta(s)$ は正則で，$s=1$ で 1 位の極をもち，留数は 1 である．

（2）　m を自然数とする．$\zeta(s)$ の $s = 1-m$ での値は

$$\zeta(1-m) = -\frac{B_m}{m}$$

である．

証明　(1) はすでに示してあるので，(2) を示す．

$s=1-m$ のとき，(5.4) 式において M を $M \geq m$ にとれば $(1-m)_M=0$ となり，右辺の積分項が消える．すなわち $\zeta(1-m)$ がある有限和として表されていることになる．これを簡潔な形に書くのが目標である．

(5.4) 式において $s=1-m$, $M=m$ とすると，

$$\zeta(1-m) = -\frac{1}{m}+\frac{1}{2}+\sum_{k=1}^{m-1}\frac{B_{k+1}}{(k+1)!}\cdot(1-m)(2-m)\cdots(k-m). \tag{5.6}$$

$m=1$ ならば右辺の和の項はなく，

$$\zeta(0) = -1+\frac{1}{2} = -\frac{1}{2} = -B_1.$$

$m \geq 2$ とする．ここで，$(1-m)(2-m)\cdots(k-m) = (-1)^k k!\binom{m-1}{k}$, および $\frac{1}{k+1}\binom{m-1}{k} = \frac{1}{m}\binom{m}{k+1}$，また $(-1)^k B_k = B_k$ $(k \geq 2)$ を用いて

$$\begin{aligned}
&\sum_{k=1}^{m-1}\frac{B_{k+1}}{(k+1)!}\cdot(1-m)(2-m)\cdots(k-m)\\
&= \sum_{k=1}^{m-1}(-1)^k\frac{B_{k+1}}{k+1}\binom{m-1}{k}\\
&= \frac{1}{m}\sum_{k=1}^{m-1}(-1)^k\binom{m}{k+1}B_{k+1}\\
&= \frac{1}{m}\sum_{k=2}^{m}(-1)^{k-1}\binom{m}{k}B_k\\
&= -\frac{1}{m}\sum_{k=2}^{m}\binom{m}{k}B_k.
\end{aligned}$$

よって，(5.6) 式の右辺は，（$B_0=1$, $B_1=1/2$ より）

$$-\frac{1}{m}\sum_{k=0}^{m}\binom{m}{k}B_k+1$$

に等しい．ここで，ベルヌーイ数を定義する漸化式 (1.2)（4 ページ）より

$$\sum_{k=0}^{m-1}\binom{m}{k}B_k = m$$

であるので，$k=m$ の項だけが残り，

$$\zeta(1-m)=-\frac{B_m}{m}$$

を得る． ∎

注意 5.5 (2) の値をはじめて与えたのは Euler ([24], また Weil[6][90] も参照) である．系 4.12（61 ページ）で与えた，リーマンゼータ関数の正の偶数点での値

$$\zeta(2k)=\frac{(-1)^{k-1}}{2}\frac{B_{2k}}{(2k)!}(2\pi)^{2k} \qquad (k\in\mathbf{N})$$

もやはり Euler がはじめて計算した（上記文献参照）．奇数点での値について知られていることは少ない．$\zeta(2k+1)$ もすべて超越数であろうと予想されている[7]が，わずかに $\zeta(3)$ が無理数であることが Apéry [8][3] によって証明されているにすぎない．

注意 5.6 べき乗和の公式はオイラー・マクローリンの和公式（定理 5.1）を用いても得られる．上の $\sum_{n=1}^{N} n^{m-1}$ ならば，和公式で $f(x)=x^{m-1}$，$a=1$，$b=N$ とすればよい．

[6] André Weil（1906.5.6 フランス Paris 生――1998.8.6 アメリカ Princeton 没）

[7] π が超越数（Lindemann [62]）なので $\zeta(2k)$ はすべて超越数である．

[8] Roger Apéry（1916.11.14 フランス Ruen 生――1994.12.18 フランス Caen 没）

第6章

2次体のイデアル論と2次形式

ベルヌーイ数と2次体または2次形式の類数とは密接な関係がある．これについて説明するために，2次体のイデアル論と2次形式について解説する．Gauss以来，2次体（有理数体上2次の拡大体）のイデアル論と整数係数の2元2次形式論の間に深い関係があること（ほとんど同じものであること）が知られている．これは専門家にとってはまったく明らかなことであるにもかかわらず，なぜかこれについて詳しく解説した教科書はほとんどない．たいていの解説書には，記述の単純な，いわゆる極大整環（(全) 整数環ともいう）のイデアル論との対応の部分のみ書いてある．これは，はなはだ残念なことである．これでは2次形式の全貌にはせまり得ないばかりでなく，時として誤解を生む一因にもなっているからである．第10章で，概均質ベクトル空間の L 関数とベルヌーイ数の関係を解説するために，これが必要になるので，よい機会であるからここで解説を試みたい．

6.1 2次形式

整数係数の2元2次形式というのは，整数 a, b, c と変数 x, y についての2次の斉次式

$$Q(x,y) = ax^2 + bxy + cy^2$$

のことである．特に a, b, c が互いに素（すなわち最大公約数が1）のとき $Q(x,y)$ を原始的という．ここで行列を用いて

$$S = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$$

とおけば

$$Q(x,y) = (x,y)S\begin{pmatrix} x \\ y \end{pmatrix}$$

である．このように表したほうがいろいろわかりやすい．S のように対角成分が整数で，それ以外の成分が半整数[1]（2 倍すると整数）となるような対称行列を一般に半整数対称行列という．2 次の半整数対称行列の全体を L^* と書くことにする．すなわち

$$L^* = \left\{ \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} ;\ a,b,c \in \mathbf{Z} \right\}.$$

これはもちろん整数係数の 2 元 2 次形式の全体と 1 対 1 に対応している．また，対応する 2 次形式 $(x,y)S\begin{pmatrix} x \\ y \end{pmatrix}$ が原始的なとき，S も原始的であるという．行列式が 1 の整数行列のなす群（モジュラー群）

$$SL_2(\mathbf{Z}) = \{g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbf{Z}); ad-bc=1\}$$

を考える．群 $SL_2(\mathbf{Z})$ は L^* に

$$L^* \ni S \mapsto {}^t\gamma S\gamma \in L^* \qquad (\gamma \in SL_2(\mathbf{Z}))$$

で作用する．この作用で写りあう L^* の元，または対応する 2 次形式を互いに同値ということにする．（群 $SL_2(\mathbf{Z})$ を少し広げて $GL_2(\mathbf{Z})$ つまり，$ad-bc=1$ という条件を $ad-bc=\pm 1$ にかえたものの作用を考えることもある．この場合と特に区別したいときは $SL_2(\mathbf{Z})$ に関する同値を「真に」同値と呼ぶこともある．本書では $SL_2(\mathbf{Z})$ による同値類のみ考えるので，単に同値と呼ぶ.）

通常，$-\det(2S) = b^2-4ac$ のことを 2 次形式の判別式という．これを $D(S)$

[1] ここで半整数というときは，整数も含めている．

と書くことにする．$SL_2(\mathbf{Z})$ の作用は判別式を不変に保つ．判別式 D が平方数（整数の 2 乗になるもの，たとえば 0, 1, 4, 9 など）のものは，やや例外的なので，以下この章では特に断らない限り D はこれ以外の数，すなわち平方数以外の数とする．このような D を固定して $L^*(D) = \{S \in L^*; D(S) = D\}$ とおくと，$L^*(D)$ 内での $SL_2(\mathbf{Z})$ 同値類の個数は有限であることが知られている．これを判別式 D の 2 次形式の類数という．これを $h(D)$ と書くことにする．（類数が有限であることの証明や類数の具体的な公式は後で述べる．）

6.2　2 次体の整環

さて，対応する 2 次体論を復習しなければならないが，これについては述べてある本も多いので，なるべく簡単にすませる．また 2 次体のイデアル論よりも 2 次形式の視点を主体に述べるので，そのために記述がかえって煩雑になった部分もあるが，現在このような本があまり見あたらないので，それなりの意義はあるのではないかと考える．

まず，m が平方数でないときに，$K = \mathbf{Q}(\sqrt{m})$ を 2 次体というのであった．また，$m > 0$ のとき K は実 2 次体，$m < 0$ のときは虚 2 次体という．m に平方因子があれば平方根の外に出せるから，m は平方因子をもたない整数としてよい．以下そのように仮定する．この体 K の元 α で $\alpha^2 + b\alpha + c = 0$ が適当な有理整数（普通の整数）b, c について成り立つものを K の整数という．K の整数全体 $\mathfrak{O}_{\max}$ は環をなし，

$$\omega = \begin{cases} \frac{1+\sqrt{m}}{2} & m \equiv 1 \bmod 4 \text{ の場合}, \\ \sqrt{m} & \text{それ以外の場合} \end{cases} \tag{6.1}$$

とおくと，$\mathfrak{O}_{\max} = \mathbf{Z} + \mathbf{Z}\omega$ となる．環 $\mathfrak{O}_{\max}$ を $\mathbf{Q}(\sqrt{m})$ の極大整環，または全整数環という．（単に整数環という場合もあるが，あとで極大整環より小さい環を考えて，それも整数環，ないしは整環と呼ぶので，区別するために極大整環というのである．max というのはあとから考える整環の中で一番大きいという意味である．また極大整環というのはそれ以上本当に大きい整環がないという意味であり，いまの場合，一番大きいといっても同じである．最大整環といわ

ずに極大整環というのは，多元環の整数論では極大整環はあるが最大整環は存在しないという事実からくる，用語の習慣による.）

K から K への $\mathbf{Q}$ ベクトル空間としての線形写像 ρ を $\rho(a+b\sqrt{m}) = a-b\sqrt{m}$ $(a, b \in \mathbf{Q})$ と定義するとこれは体としての自己同型写像になる．K の元 α について $N(\alpha) = \alpha\rho(\alpha), Tr(\alpha) = \alpha + \rho(\alpha)$ と書き，前者を元 α のノルム，後者をトレースという．$D_K = (\omega - \rho(\omega))^2 = Tr(\omega)^2 - 4N(\omega)$ とおいて，これを K の判別式，または基本判別式という．具体的には $m \equiv 1 \bmod 4$ ならば $D_K = m$，それ以外では $D_K = 4m$ である．

極大整環 $\mathfrak{O}_{\max}$ は一般に単項イデアル環でも一意素元分解環でもなく，$\mathfrak{O}_{\max}$ の元の素因数分解というものはうまく定義できないことが知られている．しかし，元のかわりに $\mathfrak{O}_{\max}$ のイデアルを考えると，$\mathfrak{O}_{\max}$ の任意のイデアルは素イデアルの積に一意的に分解される．この事実は整数全体のなす環 $\mathfrak{O}_{\max}$ がデデキント環であることによる．しかし，整数全体ではなくて $\mathfrak{O}_{\max}$ の部分環を考えることが有用なこともある．たとえば 2 次形式との対応では，このような部分環を考えるのは避けられない．しかし，部分環は一般にはデデキント環ではないので素イデアル分解の一意性は成り立たない点は注意が必要である[2]．

さて，$\mathfrak{O}_{\max}$ の 1 を含む部分環 $\mathfrak{O}'$ はアーベル群の基本定理により $\mathbf{Z}$ 上の自由加群であるが，このうち階数が 2 のものを単に整環と呼ぶ．これをすべて求めよう．

補題 6.1　ω は (6.1) 式のとおりとする．任意の自然数 f に対し，

$$\mathfrak{O}_f = \mathbf{Z} + f\omega\mathbf{Z}$$

とおくと，これは $\mathbf{Q}(\sqrt{m})$ の整環である．逆に $\mathbf{Q}(\sqrt{m})$ の任意の整環 $\mathfrak{O}'$ はある自然数 f に対して，$\mathfrak{O}' = \mathfrak{O}_f$ となる．

証明　$\mathfrak{O}_f$ が整環であることは容易に確かめられる．逆に，$\mathfrak{O}'$ を整環とすると，階数 2 ということから $\mathfrak{O}'$ は $\mathbf{Z}$ に属さない元を含む．よって適当な整数 a および 0 でない整数 b があって $a + b\omega \in \mathfrak{O}'$．このとき $1 \in \mathfrak{O}'$ より $b\omega \in \mathfrak{O}'$ である．$b\omega \in \mathfrak{O}'$ となる正の b のうちで最小のものを f とすると，他のこのような b はすべて f で割り切れる．実際，$b\omega \in \mathfrak{O}'$ とし，b を f で割って

[2]たとえば Lang [60] の旧版の p. 91 には誤って一意性が成り立つと書いてあった．改版ではその部分は削除されている．

$b = fx + b_0$, $x \in \mathbf{Z}$, $0 \le b_0 < f$ と書くと，$b_0\omega = (b - fx)\omega = b\omega - x(f\omega) \in \mathfrak{O}'$. これと f の最小性から $b_0 = 0$，すなわち b は f で割り切れる．以上により，$\mathfrak{O}' = \mathbf{Z} + f\omega\mathbf{Z} = \mathfrak{O}_f$ となる． ∎

整環 $\mathfrak{O}_f$ は f が異なればもちろん異なる環になる．この環は

$$\mathfrak{O}_f = \mathbf{Z} + f\mathfrak{O}_{\max}$$

とも書き表される．f を整環 $\mathfrak{O}_f$ の導手という．整環の導手が 1 であることと $\mathfrak{O}_f$ が極大整環であることは同値である．整環 $\mathfrak{O}_f$ の判別式を $f^2 D_K$ と定義する．

慣用により零イデアル（0 のみからなるイデアル）以外の $\mathfrak{O}_f$ のイデアル $\mathfrak{a}$ のことを単に $\mathfrak{O}_f$ のイデアルと呼ぶ．$\mathfrak{a}$ は $\mathfrak{O}_f$ の部分加群だから，$\mathbf{Z}$ 上の自由加群だが，$\mathfrak{O}_f$ 加群でもあるから，階数は 2 である．よって $\mathfrak{O}_f/\mathfrak{a}$ は有限環である．この元の個数を $\mathfrak{a}$ のノルムといい $N(\mathfrak{a})$ と書く．$\mathfrak{O}_f$ のイデアル $\mathfrak{a}$ の自由 $\mathbf{Z}$ 加群としての基底をもっと詳しく記述してみよう．ある整数 $l > 1$ と $\mathfrak{O}_f$ のイデアル $\mathfrak{b}$ を用いて $\mathfrak{a} = l\mathfrak{b}$ という形には書き表せないようなイデアル $\mathfrak{a}$ のことを原始的イデアルという．

補題 6.2　$\mathfrak{O}_f$ のイデアル $\mathfrak{a}$ に対して，正の整数 a, e と $-a/2 \le d < a/2$ となる整数 d で

$$\mathfrak{a} = \mathbf{Z}a + \mathbf{Z}(d + ef\omega)$$

となるものが一意的に存在する．さらに，$\mathfrak{a}$ が原始的イデアルならば，上で $e = 1$ となる．また原始的イデアル $\mathfrak{a}$ のノルムは a である．

証明　しばらくは $\mathfrak{a}$ は $\mathfrak{O}_f$ の任意のイデアルとし，原始的とは仮定しない．$\mathfrak{O}_f/\mathfrak{a}$ が有限加群であるから，1 の何倍かが $\mathfrak{a}$ に含まれ，$\mathfrak{a} \cap \mathbf{Z} \ne 0$ である．$\mathfrak{a}$ に含まれる最小の有理正整数 a をとろう．すなわち a は $\mathbf{Z}$ のイデアル $\mathfrak{a} \cap \mathbf{Z}$ の正の生成元である．一方で，$x + yf\omega \in \mathfrak{a}$ となる整数 x が存在するような最小の正整数 y を e と書き，整数 d について $d + ef\omega \in \mathfrak{a}$ とすると，

$$\mathfrak{a} = \mathbf{Z}a + \mathbf{Z}(d + ef\omega)$$

となる．実際，$x + yf\omega \in \mathfrak{a}$ ならば，y は e で割り切れる．もしそうでなければ，$(d + ef\omega)$ の何倍かを引けば，y を e で割った余りが $f\omega$ の係数に現れ，e の最小性に反するからである．ゆえに，$(x + yf\omega) - z(d + ef\omega) \in \mathbf{Z} \cap \mathfrak{a}$ となる整数 z が存在するが，この式は a の整数倍である．よって示された．以上で $-a/2 \le d < a/2$ としてよいのは明らかであるし，またこのようにとれば，a,

d, e はイデアル $\mathfrak{a}$ に対して一意的に定まる．このとき，$(a, d+ef\omega)$ をイデアル $\mathfrak{a}$ の標準基底と呼ぶことにする．$\mathfrak{a} = l(\mathbf{Z}a + \mathbf{Z}(d+ef\omega))$ と書いて，a, d, e は互いに素（すなわち a, d, e の最大公約数が 1）であるとしてもよい．このとき $\mathfrak{b} = \mathbf{Z}a + \mathbf{Z}(d+ef\omega)$ とおくとこれは明らかに $\mathfrak{O}_f$ の原始的なイデアルである．逆に原始的なイデアルの標準基底では，a, d, e は互いに素である．

さて，原始的イデアルについては上の記号で必然的に $e=1$ となり，

$$\mathfrak{b} = \mathbf{Z}a + \mathbf{Z}(d+f\omega)$$

と書けることを示す．実際，原始的なイデアル $\mathfrak{b}$ については，前のように標準基底をとって $\mathfrak{b} = \mathbf{Z}a + \mathbf{Z}(d+ef\omega)$ と表示するとき，$f\omega\mathfrak{b} \subset \mathfrak{b}$ であることより，$af\omega \in \mathfrak{b}$ である．よって e の取り方により a は e で割り切れる．同様に $(d+ef\omega)f\omega = df\omega + ef^2\omega^2 \in \mathfrak{b}$ であり，これを $x+yf\omega (x, y \in \mathbf{Z})$ と書くと y は e で割り切れるはずである．しかし $\omega^2 \in \mathfrak{O}_{\max}$ だから，$f^2\omega^2 \in \mathfrak{O}_f$ であり，$ef^2\omega^2 \in e\mathfrak{O}_f$，よって d も e で割り切れる．よってもし $e>1$ ならば，a, d, e の最大公約数が e となり，原始的という仮定に反する．特に $\mathfrak{a}$ のノルムは a である．　■

注意 6.3　原始的なイデアルのノルム a と f は互いに素とは限らない．たとえば，$\mathbf{Z}5 + \mathbf{Z}5\sqrt{2}$ は，2次体 $K = \mathbf{Q}(\sqrt{2})$ の導手 5 の整環 $\mathfrak{O}_5$ のイデアルとしては原始的であり，ノルム 5 をもつ．$\mathbf{Z}5 + \mathbf{Z}5\sqrt{2} = 5(\mathbf{Z} + \mathbf{Z}\sqrt{2})$ と書けるが，$\mathbf{Z} + \mathbf{Z}\sqrt{2}$ は $\mathfrak{O}_5$ のイデアルではない（部分集合ではない）からである．

さて，以上でイデアルの標準基底の形はわかったが，逆に $M = \mathbf{Z}a + \mathbf{Z}(d+f\omega)$ なる加群を与えても，これはかなり特別な条件がない限り $\mathfrak{O}_f$ のイデアルにはならない．これがイデアルになるための条件を書こう．

補題 6.4　加群 $M = \mathbf{Z}a + \mathbf{Z}(d+f\omega)$ が $\mathfrak{O}_f$ のイデアルになるための必要十分条件は，

$$a | N(d+f\omega)$$

なることである．これはまた，$b = Tr(d+f\omega)$ とおくとき，整数 c で

$$b^2 - f^2 D_K = 4ac$$

となるものが存在することと同値である．

証明　このためには $f\omega M \subset M$ のための条件を求めればよい．$f\omega \cdot a = (-d)a + a(d+f\omega) \in M$ である．$f\omega(d+f\omega)$ であるが，

$$f\omega(d+f\omega)=(d+Tr(f\omega))(d+f\omega)-N(d+f\omega) \tag{6.2}$$

なので，これが M の元であるための必要十分条件は $N(d+f\omega)$ が a で割り切れることである．また，

$$\begin{aligned}b^2-f^2D_K &= (2d+fTr(\omega))^2-f^2(Tr(\omega)^2-4N(\omega))\\ &= 4(d^2+dfTr(\omega)+f^2N(\omega))\\ &= 4N(d+f\omega)\end{aligned}$$

であるので，これはまた

$$b^2-f^2D_K=4ac$$

となる整数 c が存在することであるといえる． ∎

さて，$\mathfrak{O}_f$ のイデアル $\mathfrak{a}$ について，環 $\{x\in K; x\mathfrak{a}\subset\mathfrak{a}\}$ は $\mathfrak{O}_{\max}$ の $\mathfrak{O}_f$ を含む部分環であり，よってある f の約数 f' により $\mathfrak{O}_{f'}$ と書ける．これが $\mathfrak{O}_f$ と一致するとき，すなわち $f=f'$ のとき $\mathfrak{a}$ を $\mathfrak{O}_f$ の固有イデアルという．$\mathfrak{O}_f$ の原始的なイデアルが $\mathfrak{O}_f$ の固有イデアルであるための条件を求めよう．

補題 6.5 $\mathfrak{O}_f$ の原始的イデアル $\mathfrak{a}$ について，$\mathfrak{a}=\mathbf{Z}a+\mathbf{Z}(d+f\omega)$ を標準基底による表示とし，整数 b, c を補題 6.4 のように定める．このとき，$\mathfrak{a}$ が $\mathfrak{O}_f$ の固有イデアルであるための必要十分条件は a, b, c が互いに素であることである．

証明 これを証明するために f の約数 f' について $\mathfrak{a}$ が $\mathfrak{O}_{f'}$ 加群でもあるための条件を考える．もし $\mathfrak{a}$ が $\mathfrak{O}_{f'}$ 加群ならば，$af'\omega\in\mathfrak{a}$ より，$af'\omega=xa+y(d+f\omega)$ と書けるが，ω の係数を見て $a=y(f/f')$，これと $xa+yd=0$ より $d=-x(f/f')$，よって $a,d\in(f/f')\mathbf{Z}$ である．また，$\mathfrak{a}$ の標準基底 $(a, d+f\omega)$ に対して補題 6.4 のように c を定めるとき，その証明中の (6.2) 式に f'/f をかけて

$$f'\omega(d+f\omega)=(f'd/f+f'Tr(\omega))(d+f\omega)-acf'/f$$

となる．よって，$f'\omega(d+f\omega)\in\mathfrak{a}$ ならば，d, $c\in(f/f')\mathbf{Z}$ となる．逆に a, c, $d\in(f/f')\mathbf{Z}$ ならば $\mathfrak{a}$ が $\mathfrak{O}_{f'}$ 加群になるのは，上の式から明らかである．

以上によって，a, c, $d\in(f/f')\mathbf{Z}$ が $\mathfrak{a}$ が $\mathfrak{O}_{f'}$ 加群となるための必要十分条件となる．ここで，$b=Tr(d+f\omega)$ とおけば，a, c, $d\in(f/f')\mathbf{Z}$ なる条件は a, b, $c\in(f/f')\mathbf{Z}$ という条件と同値である．実際，$d\in(f/f')\mathbf{Z}$ ならば $b\in(f/f')\mathbf{Z}$ は明らかである．逆に，$a,b,c\in(f/f')\mathbf{Z}$ とする．$t=f/f'$ とおく．$t^2|ac=N(d+f\omega)=d^2+dfTr(\omega)+f^2N(\omega)$ と $t^2|f^2$ より，$t^2|d(d+fTr(\omega))$

である．一方 $t|b = d + d + fTr(\omega)$．次の補題により，この 2 つから $t|d$ が結論できる．

補題 6.6　$a, b, t \in \mathbf{Z}$ について，$t|(a+b)$, $t^2|ab$ ならば $t|a$, $t|b$ である．

これは次のように証明する．2 次多項式 $(x - a/t)(x - b/t) = x^2 + mx + n$ を考えると，条件より $m, n \in \mathbf{Z}$ である．これの根 p/q（有理数）が整数であることをいう．p, q は互いに素としてよいが，このとき，$p^2 + mpq + nq^2 = 0$ より q は p を割らなければならない．すなわち $q = \pm 1$ で，p/q は整数である．よって $a/t, b/t$ は整数である．∎

これで，a, b, $c \in (f/f')\mathbf{Z}$ ならば a, c, $d \in (f/f')\mathbf{Z}$ なることが証明された．したがって，$\mathfrak{a}$ が $\mathfrak{O}_{f'}$ 加群であるための必要十分条件は a, b, $c \in (f/f')\mathbf{Z}$ となることである．$\mathfrak{a}$ が $\mathfrak{O}_f$ の固有イデアルであるとは，$\mathfrak{a}$ が $\mathfrak{O}_{f'}$ 加群となるような f の真の約数 f' が存在しないことであるから，言い換えると，a, b, c の最大公約数が 1 であることである．

補題 6.7　任意の 2 次形式 $ax^2 + bxy + cy^2$ について，その判別式が平方数でなければ，ある 2 次体 K と自然数 f で $b^2 - 4ac = f^2 D_K$ となるものが存在する．

証明　$b^2 - 4ac$ はいつでも $0 \bmod 4$ または $1 \bmod 4$ である．これを奇数 f_0 と平方因子をもたない奇数 D, 0 以上の整数 e について $b^2 - 4ac = 2^e f_0^2 D$ と書く．$e = 0$ ならば $D \equiv 1 \bmod 4$, $D \neq 1$ であるから，2 次体 $K = \mathbf{Q}(\sqrt{D})$ が $D_K = D$ となり，これと $f = f_0$ が求めるものである．$e \neq 0$ ならば $e \geq 2$ である．e が奇数ならば，K として $\mathbf{Q}(\sqrt{2D})$ をとれば $D_K = 8D$ となり，$f = 2^{(e-3)/2} f_0$ とおけばよい．e が偶数ならば，$K = \mathbf{Q}(\sqrt{D})$ とすれば，$D \equiv 1 \bmod 4$ のときは $D_K = D$ なので $f = 2^{e/2} f_0$ とおき，$D \equiv 3 \bmod 4$ ならば $D_K = 4D$ なので $f = 2^{(e-2)/2} f_0$ とおけばよい．∎

この補題から考えても，2 元 2 次形式と 2 次体には深い関係があることが推察される．2 次体の原始的な固有イデアル $\mathfrak{a}$ に対して，補題 6.4 の a, b, c を用いて，2 次形式を

$$Q_{\mathfrak{a}}(x, y) = ax^2 + bxy + cy^2$$

と定義する．これは

$$Q_{\mathfrak{a}}(x,y) = N(\mathfrak{a})^{-1}N(xa + y(d + f\omega)) = aN(x + y\frac{d+\omega}{a})$$

と書いても同じである．ここで $a,\ d+f\omega$ は $\mathfrak{a}$ の基底であるから，$\mathfrak{a} = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ と他の基底を用いて，2 次形式

$$Q_{\omega_1,\omega_2}(x,y) = N(\mathfrak{a})^{-1}N(x\omega_1 + y\omega_2)$$

を定義すると，もとの $Q_{\mathfrak{a}}(x,y)$ とどのような関係にあるかが当然気になるところである．ここで，ともに $\mathfrak{a}$ の基底であることより，ある $A \in GL_2(\mathbf{Z})$ により，$(\omega_1,\omega_2) = (a, d + f\omega)A$ となり，容易に

$$Q_{\mathfrak{a}}((x,y)\,{}^tA) = Q_{\omega_1,\omega_2}(x,y)$$

となることがわかる．さらに $\det(A) = 1$ であれば，2 つの 2 次形式は前に定義した意味で同値である．よって，ここで A として $\det(A) = 1$ のものがとれる条件を見てみよう．

$$\det\begin{pmatrix} \omega_1 & \omega_2 \\ \rho(\omega_1) & \rho(\omega_2) \end{pmatrix} = \det\begin{pmatrix} a & d + f\omega \\ a & d + f\rho(\omega) \end{pmatrix}\det(A)$$

であるから，

$$\begin{aligned} af(\rho(\omega) - \omega)\det(A) &= \omega_1\rho(\omega_2) - \omega_2\rho(\omega_1) \\ &= N(\omega_1)(\rho(\omega_2/\omega_1) - \omega_2/\omega_1). \end{aligned}$$

よって $af > 0$ であるから

$$\omega_2/\omega_1 - \rho(\omega_2/\omega_1) \in N(\omega_1)^{-1}\sqrt{D_K}\mathbf{Q}_+$$

（ただし $\mathbf{Q}_+$ は正の有理数の集合）が $\det(A) = 1$ になるための必要十分条件である．ただし，ここで D_K の平方根の選び方は $\sqrt{D_K} = \omega - \rho(\omega) = \sqrt{m}$ または $2\sqrt{m}$ としている．

さて，さらに一般に K の 2 つの基底 (ω_1,ω_2) と (ω_3,ω_4) について，2 次形式として

$$N(x\omega_1 + y\omega_2) = N(x\omega_3 + y\omega_4)$$

となると仮定する．すると $x,\ y$ の多項式として各係数を比較すると $N(\omega_1) = N(\omega_3)$, $N(\omega_2) = N(\omega_4)$，$\omega_1\rho(\omega_2) + \rho(\omega_1)\omega_2 = \omega_3\rho(\omega_4) + \rho(\omega_3)\omega_4$ がわかる．最後の式の左辺を $N(\omega_1)$, 右辺を $N(\omega_3)$（$= N(\omega_1)$）で割って $Tr(\omega_2/\omega_1) = Tr(\omega_4/\omega_3)$，また $N(\omega_2/\omega_1) = N(\omega_4/\omega_3)$．よって ω_2/ω_1 と ω_4/ω_3 の $\mathbf{Q}$ 上の

最小多項式は等しい．よって，$\alpha = \omega_2/\omega_1$ とすると $\omega_4/\omega_3 = \alpha$ または $\rho(\alpha)$ である．さらに

$$\omega_2/\omega_1 - \rho(\omega_2/\omega_1),\ \omega_4/\omega_3 - \rho(\omega_4/\omega_3) \in N(\omega_1)^{-1}\sqrt{D_K}\mathbf{Q}_+$$

と仮定すると，$\alpha \notin \mathbf{Q}$ より $\alpha - \rho(\alpha) = -(\rho(\alpha) - \alpha) \neq 0$ だから，$\omega_4/\omega_3 = \alpha = \omega_2/\omega_1$ がいえる．

$\mathfrak{O}_f$ の 2 つの固有イデアル $\mathfrak{a}$ と $\mathfrak{b}$ に対して，$N(\alpha) > 0$ なる K の元が存在して $\mathfrak{a} = (\alpha)\mathfrak{b}$ となるとき，$\mathfrak{a}$ と $\mathfrak{b}$ は狭義の意味で同値であるという．

ここで $N(\alpha) > 0$ という条件は，K が虚 2 次体ならば自動的に成り立ち，K が実 2 次体ならば，必要ならば α を $-\alpha$ に置き換えて，$N(\alpha) > 0$ という条件を $\alpha > 0$ かつ $\rho(\alpha) > 0$ という条件に書き換えてもよい．むしろこちらのほうが同値の普通の（一般論に適合した）定義であるが，簡略に上のように述べてみた．一方で，2 次体のイデアルで，$\mathfrak{a} = \alpha\mathfrak{b}$ となる $\alpha \in K^\times$ があるとき，$\mathfrak{a}$ と $\mathfrak{b}$ は広義の意味で同値であるという．実際は，広義の同値類の個数を類数ということが多いが，2 次形式との関係からいえば狭義の同値類を用いるほうが自然である．なお，K が虚 2 次体ならば，広義と狭義は一致する．以下特に断らない限り，イデアルの同値は狭義の同値を意味することにする．

$\mathfrak{O}_f$ の固有イデアル全体を狭義（広義）の同値類に分けたときの同値類の個数を $\mathfrak{O}_f$ の狭義（広義）の類数という．さて，K を 2 次体とし，D_K を K の基本判別式とする．また，f を自然数とする．$\mathfrak{O}_f$ の原始的な固有イデアル $\mathfrak{a} = \mathbf{Z}a + \mathbf{Z}(d + f\omega)$ から 2 次形式の集合への写像を，$b = 2d + fTr(\omega)$，$N(d + f\omega) = ac$ によって b, c を定め，$f_{\mathfrak{a}}(x, y) = ax^2 + bxy + cy^2$ を対応させることにより定める．この写像は原始的な固有イデアルから原始的 2 次形式の上への 1 対 1 写像を引き起こすわけではない．イデアル $\mathfrak{a}$ の表示において，d が $\bmod a$ での不定性をもつことがその事情の原因である．つまり，上の構成を逆に原始的 2 次形式から出発して，与えられた a, b, c に対して d を $d = (b - fTr(\omega))/2$ で定義できるが，ここで d は $-a/2 \leq d < a/2$ となるとは限らないので，イデアルと 2 次形式が 1 対 1 とはいえないのである．しかし，次が成り立つ．

命題 6.8　上の写像は，K が虚 2 次体，すなわち $D_K < 0$ のときは $\mathfrak{O}_f$ の原始的な固有イデアルの同値類の集合から，判別式が f^2D_K の原始的な正定値 2 次形式の同値類の集合の上への 1 対 1 写像を引き起こす．また K が実 2 次体，

すなわち $D_K > 0$ のときには同じく，$\mathfrak{O}_f$ の原始的な固有イデアルの同値類の集合から，判別式が f^2D_K の原始的な不定値 2 次形式の同値類の集合の上への 1 対 1 対応を引き起こす．

証明 $\mathfrak{O}_f$ の原始的な固有イデアルから，a, b, c を前のように定めるとこれらの最大公約数 $(a,b,c)=1$ であったから，$f_{\mathfrak{a}}(x,y)=ax^2+bxy+cy^2$ は原始的な 2 次形式であり判別式は f^2D_K である．より直接的には

$$f_{\mathfrak{a}}(x,y)=ax^2+bxy+cy^2=a^{-1}N(ax+(d+f\omega)y)$$

と書けることが容易に確かめられる．逆に原始的 2 次形式 $ax^2+bxy+cy^2$ を 1 つとる．これが正定値ならば自動的に $a>0$ である．不定値と仮定すると $a<0$ かもしれないが，同値なものに取り替えて $a>0$ にできる．これは次のようにする．$a<0$ と仮定する．$4a(ax^2+bxy+cy^2)=(2ax+by)^2+(4ac-b^2)y^2$ であるが，不定値の仮定より $4ac-b^2<0$ である．y を固定すると，x を適当に選んで，$2ax+by$ は $\mathrm{mod}\,2a$ の代表系の元としてよいから，$|2ax+by|\leq|a|$ とできる．よって，$|a|/\sqrt{b^2-4ac}<y$ ととれば，x を適当に選んで $(2ax+by)^2-(b^2-4ac)y^2<0$ とできる．すなわち $(x,y)\in\mathbf{Z}^2$ で $ax^2+bxy+cy^2>0$ となるものがある．x, y を最大公約数で割っても，この性質はかわらないから，(x,y) は互いに素としてよい．よって (x,y) を第 1 行とする $SL_2(\mathbf{Z})$ の元 A がとれて，$A\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}{}^tA$ の (1,1) 成分が正としてよい．よって示された．

以下 $a>0$ との仮定のもとで考える．判別式が $b^2-4ac=f^2D_K$ であるとき，$b=2d-fa_1=2d+fTr(\omega)$ とおくと，$(fTr(\omega))^2=f^2(D_K+4N(\omega))$ より，$fTr(\omega)\equiv f^2D_K \bmod 2$ であり，よって $b\equiv fTr(\omega) \bmod 2$，ゆえに d は整数となる．ここで，$\mathfrak{a}=\mathbf{Z}a+\mathbf{Z}(d+f\omega)$ を対応させれば 2 次形式からイデアルを定めることができるが，しかし前に述べたように $-a/2\leq d<a/2$ とは限らない．ここで，$-a/2\leq d_0=d-ak<a/2$ となるような $k\in\mathbf{Z}$ をとると $(a,d_0+f\omega)$ が標準基底であって，$ac_0=N(d_0+f\omega)$, $b_0=2d_0+fTr(\omega)$ とおくと，$f_{\mathfrak{a}}(x,y)=ax^2+b_0xy+c_0y^2$ である．ここで $b_0=b-2ak$ である．また

$$\begin{aligned} ac_0 &= N(d+f\omega-ak) \\ &= N(d+f\omega)-akTr(d+f\omega)+a^2k^2 \\ &= ac-abk+(ak)^2 \end{aligned}$$

より，$c_0=c-bk+ak^2$．よって，

$$\begin{aligned} f_{\mathfrak{a}}(x,y) &= ax^2 + (b-2ak)xy + (c-bk+ak^2)y^2 \\ &= a(x-ky)^2 + b(x-ky)y + cy^2. \end{aligned}$$

ゆえに $f_{\mathfrak{a}}(x,y)$ は最初に与えた原始的2次形式と同値である．すなわち，問題の写像は，原始的2次形式の同値類の集合の上への写像を与えている．

さて，$\mathfrak{a}$ の任意の基底 ω_1, ω_2 をとって $\mathfrak{a} = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ とし，$Q_{\omega_1,\omega_2}(x,y) = N(\mathfrak{a})^{-1}N(x\omega_1 + y\omega_2)$ とおくと，$(\omega_1\rho(\omega_2) - \rho(\omega_1)\omega_2) = \pm af(\rho(\omega) - \omega)$ であるが，この符号がプラスならば，$Q_{\omega_1,\omega_2}(x,y)$ は $Q_{\mathfrak{a}}(x,y)$ と同値であることは前に示した．さて，もし $\mathfrak{b} = \alpha\mathfrak{a}$, $N(\alpha) > 0$ ならば，$\mathfrak{b}$ の基底 $\omega_1 = \alpha a$ と $\omega_2 = \alpha(d+f\omega)$ をとると，定義より

$$\begin{aligned} Q_{\omega_1,\omega_2}(x,y) &= N(\mathfrak{b})^{-1}N(\alpha ax + \alpha(d+f\omega)y)) \\ &= a^{-1}N(x + y(d+f\omega)) = Q_{\mathfrak{a}}(x,y) \end{aligned}$$

である．また，計算すると $\omega_2/\omega_1 - \rho(\omega_2/\omega_1) = a^{-1}f(\omega - \rho(\omega))$ となり，これは $\sqrt{D_K}$ の正の有理数倍であり，上記の条件を満たすから，$Q_{\omega_1,\omega_2}(x,y)$ は $f_{\mathfrak{b}}(x,y)$ と同値である．よって，同値なイデアルは同値な2次形式に写る．

逆に $\mathfrak{a} = \mathbf{Z}a + \mathbf{Z}(d+f\omega)$ と $\mathfrak{b} = \mathbf{Z}a' + \mathbf{Z}(d'+f\omega)$ について，$Q_{\mathfrak{a}}(x,y)$ と $Q_{\mathfrak{b}}(x,y)$ が同値だと仮定しよう．このときある $A \in SL_2(\mathbf{Z})$ について，$Q_{\mathfrak{a}}((x,y)\,{}^tA) = Q_{\mathfrak{b}}(x,y)$ であり，すなわち $(a, d+f\omega)A = (\omega_1, \omega_2)$ とおくとき，

$$N(\mathfrak{a})^{-1}N(x\omega_1 + y\omega_2) = N(\mathfrak{b})^{-1}N(xa' + y(d'+f\omega))$$

である．よって，$N(\mathfrak{a})^{-1}N(\omega_1) = N(\mathfrak{b})^{-1}a'^2$ かつ，$N(x + y\omega_1^{-1}\omega_2) = N(x + a'^{-1}(d'+f\omega)y)$ であるが，$\det(A) = 1$ より，$\omega_2/\omega_1 - \rho(\omega_2/\omega_1) \in \sqrt{D_K}\mathbf{Q}_+$ であり，よって $a'^{-1}(d'+f\omega) = \omega_2/\omega_1$ となる．ゆえに $\alpha = a'/\omega_1$ とおくと，$N(\alpha) = a'^2/N(\omega_1) = N(\mathfrak{b})/N(\mathfrak{a}) > 0$ であり，$\alpha\mathfrak{a} = \alpha(\mathbf{Z}\omega_1 + \mathbf{Z}\omega_2) = \mathbf{Z}a' + \mathbf{Z}(d'+f\omega) = \mathfrak{b}$．よってイデアル $\mathfrak{a}$, $\mathfrak{b}$ は同値である． ∎

例 6.9

(1) $K = \mathbf{Q}(\sqrt{m})$, $\mathfrak{a} = \mathbf{Z}m + \mathbf{Z}\sqrt{m}$ とすると $f_{\mathfrak{a}}(x,y) = |m|^{-1}N(|m|x + y\sqrt{m}) = |m|x^2 + \mathrm{sgn}(m)y^2$.

(2) $K = \mathbf{Q}(\sqrt{-5})$ で $\mathfrak{O}_{\max} = \mathbf{Z} + \mathbf{Z}\sqrt{-5}$ のイデアル $\mathfrak{a} = 3\mathbf{Z} + (1+\sqrt{-5})\mathbf{Z}$ に対して，$f_{\mathfrak{a}}(x,y) = 3x^2 + 2xy + 2y^2$．また $\mathfrak{O}_{\max}$ 自身については $f_{\mathfrak{O}_{\max}} = x^2 + 5y^2$．実は判別式が -20 となる原始的2次形式はこれらのいずれかと同値である．

注意 6.10　以上で，原始的 2 次形式のうち，負定値のものは取り上げられていないが，これらはみな，正定値のものにマイナス 1 をかけると得られるので，除外してもそれほど問題はないといえるだろう．一方で，判別式が平方数の原始的 2 次形式も上の対応からは除外されている．このような 2 次形式は，判別式が 0 でなければいろいろな意味で非常に特殊な 2 次形式である．（たとえば単数群（自己同型群）の基本領域の体積が無限大であるなど．）ここでこういったことについて詳しく触れる余裕はないが，せっかくであるから，同値類の分類だけは述べておきたい．

$Q(x,y)=ax^2+bxy+cy^2$ を原始的 2 次形式として，$b^2-4ac=f^2$ とする．このとき，まず同値なものに取り替えて $a=0$ としてよいことをいう．実際，$a\neq 0$ ならば $ax^2+bx+c=0$ を解くと $x=(-b\pm f)/2a$ であることをヒントにして，$-b+f$ と $2a$ の最大公約数を e とし，$-b+f=x_0e$, $2a=y_0e$ で x_0, y_0 を定義すると，x_0, y_0 は互いに素であるから，$x_0w_0-y_0z_0=1$ となる w_0, $z_0\in\mathbf{Z}$ が存在する．$a\left(\frac{x_0}{y_0}\right)^2+b\left(\frac{x_0}{y_0}\right)+c=0$ より $ax_0^2+bx_0y_0+cy_0^2=0$ で，

$$\begin{pmatrix}x_0 & y_0\\ z_0 & w_0\end{pmatrix}\begin{pmatrix}a & b/2\\ b/2 & c\end{pmatrix}\begin{pmatrix}x_0 & z_0\\ y_0 & w_0\end{pmatrix}=\begin{pmatrix}ax_0^2+bx_0y_0+cy_0^2 & *\\ * & *\end{pmatrix}=\begin{pmatrix}0 & *\\ * & *\end{pmatrix}$$

となり，同値なものへの取り替えで $a=0$ のものに帰着した．もし判別式が 0 ならば，b も同時に 0 になり，原始的であることより，$c=\pm1$ である．2 次形式 y^2 と $-y^2$ は同値ではないことは容易にわかる．これで判別式が 0 のときの分類は終わる．以下 0 でないとする．さて，$bxy+cy^2$ をまた x^2 の係数が 0 のものに写す変換は

$$A=\pm\begin{pmatrix}c & z\\ -b & w\end{pmatrix}\in SL_2(\mathbf{Z})\ \text{かまたは}\ \pm\begin{pmatrix}1 & z\\ 0 & 1\end{pmatrix}$$

の形しかないことは実際に変換の形を書いてみればわかる．前者ならば

$${}^tA\begin{pmatrix}0 & b/2\\ b/2 & c\end{pmatrix}A=\begin{pmatrix}0 & -b(bz+cw)/2\\ -b(bz+cw)/2 & bzw+cw^2\end{pmatrix}=\begin{pmatrix}0 & -b/2\\ -b/2 & w\end{pmatrix}$$

であり，よって，$b>0$ のものを同値類の代表に選んでおいてよい．一方

$$\begin{pmatrix}1 & 0\\ z & 1\end{pmatrix}\begin{pmatrix}0 & b/2\\ b/2 & c\end{pmatrix}\begin{pmatrix}1 & z\\ 0 & 1\end{pmatrix}=\begin{pmatrix}0 & b/2\\ b/2 & c+bz\end{pmatrix}$$

であるから，c としては $\bmod b$ の代表をとればよい．ゆえに，判別式が $f^2\neq 0$ $(f>0)$ の同値類の代表は

$$\begin{pmatrix}0 & f/2\\ f/2 & c\end{pmatrix}\qquad (c=0,\ 1,\cdots,f-1)$$

としてよい（これらはもう互いに同値でないことは上の計算よりわかる）．特に判別式が平方数となる2次形式の同値類の個数は有限であることがわかった．その個数は f であり，原始的なものに限ると $\varphi(f)$ 個（$\varphi(f)$ はオイラー関数）である．平方数でない場合は次節で触れる．

注意 6.11　たとえ2次形式の同値類を $SL_2(\mathbf{Z})$ による同値類から $GL_2(\mathbf{Z})$ による同値類に変更して考えても，2次形式の同値類に広義のイデアル類（イデアルの同値類）をうまく対応させることはできない．たとえば

$$\begin{pmatrix}3 & 0\\ 0 & -1\end{pmatrix}\text{と}\begin{pmatrix}1 & 0\\ 0 & -3\end{pmatrix}$$

は $GL_2(\mathbf{Z})$ 同値でない．これは不定方程式 $a^2-3b^2=-1$ が整数解をもたないことから容易にわかる．一方，両者は $3\mathbf{Z}+\sqrt{3}\mathbf{Z}$ と $\mathbf{Z}+\mathbf{Z}\sqrt{3}$ の標準基底からつくった2次形式であるが，$\sqrt{3}(\mathbf{Z}+\mathbf{Z}\sqrt{3})=3\mathbf{Z}+\sqrt{3}\mathbf{Z}$ であるから，イデアルどうしは広義の意味では同値である．なお，この例の意味については，あとでまた述べる．

以下，2次整環の狭義の類数と広義の類数の関係，およびその2次形式との関係をもう少し明らかにしておく．まず，虚2次体では両者の概念は明らかに一致しているので，整環のイデアル類と原始的2次形式の理論は完全に同じものだと思ってよい．よって，実2次体のときが問題であるが，なるべく2次形式の視点から見るために，いま少し2次形式を調べてみよう．まず，$D_K>0$

のときに，判別式 f^2D_K の原始的 2 次形式 $ax^2+bxy+cy^2$ において，必要ならば同値な 2 次形式に取り替えて，$a>0,\ c<0$ としておいてよいことをいっておく．まず同値な 2 次形式の中で x^2 の係数の絶対値 $|a|$ が最小になるものをとる．このとき $(x,y)\to(y,-x)$ なる変換をすれば x^2 の係数と y^2 の係数が入れ替わることを考えれば，$|a|\le|c|$ であるのは明らかである．さらに適当な整数 $m\in\mathbf{Z}$ について，$\sqrt{b^2-4ac}-2|a|<b-2ma<\sqrt{b^2-4ac}$ とできるので，$(x,y)\to(x-my,y)$ なる変換を考えればもとの 2 次形式と同値な 2 次形式 $ax^2+bxy+cy^2$ で

$$0<\sqrt{b^2-4ac}-b<2|a|\le 2|c|$$

なるものがとれる．このとき実は $ac<0$ となっている．実際

$$\left|\frac{\sqrt{b^2-4ac}-b}{2c}\right|<\frac{2|c|}{|2c|}=1,$$

$$\left|\frac{\sqrt{b^2-4ac}+b}{2c}\right|=\left|\frac{-4ac}{2c(\sqrt{b^2-4ac}-b)}\right|=\frac{2|a|}{\sqrt{b^2-4ac}-b}>1.$$

よって，$0<-b+\sqrt{b^2-4ac}<|b+\sqrt{b^2-4ac}|$ である．したがって $-b+\sqrt{b^2-4ac}<b+\sqrt{b^2-4ac}$ かまたは $b+\sqrt{b^2-4ac}<b-\sqrt{b^2-4ac}$ であるが，後者は $\sqrt{b^2-4ac}>0$ に矛盾するから結局，前者の式より $0<b$ となる．すなわち $b^2<b^2-4ac$ であり，$ac<0$ が結論される．必要なら $(x,y)\to(y,-x)$ と変換して，$a>0,\ c<0$ としてもよい．

さて，$a>0,\ c<0$ という仮定のもとで，2 次形式 $ax^2+bxy+cy^2$ と $-cx^2-bxy-ay^2$ の関係を考える．

補題 6.12

（1） 判別式 $f^2D_K>0$ の 2 つの原始的 2 次形式

$$Q_1(x,y)=ax^2+bxy+cy^2 \qquad (a>0, c<0 \text{ と仮定}),$$
$$Q_2(x,y)=-cx^2-bxy-ay^2$$

に対応する狭義のイデアル類を代表する $\mathfrak{O}_f$ の原始的な固有イデアルを $\mathfrak{a}$ と $\mathfrak{b}$ とすると，$\mathfrak{a}$ と $\mathfrak{b}$ は広義の意味で同値である．

（2） Q_1 と Q_2 が 2 次形式の意味で同値になる（あるいは同じことだが，$\mathfrak{a}$ と $\mathfrak{b}$ が狭義の意味で同値になる）ための必要十分条件は $N(\epsilon)=-1$ となる $\epsilon\in\mathfrak{O}_f$ が存在することである．

証明　$Q_1(x,y)$ と $Q_2(x,y)$ に対応する狭義イデアル類の代表 $\mathfrak{a}, \mathfrak{b}$ はそれぞれ次のようにとれる．

$$\mathfrak{a} = \mathbf{Z}a + \mathbf{Z}(d + f\omega),$$
$$\mathfrak{b} = \mathbf{Z}c + \mathbf{Z}(d_2 + f\omega).$$

ただし，$b = 2d + fTr(\omega)$, $-b = 2d_2 + fTr(\omega)$ としている．よって，$d_2 = -d - fTr(\omega)$ であり，$d_2 + f\omega = -d - f\rho(\omega)$ であるから，$\mathbf{Z}(d_2 + f\omega) = \mathbf{Z}(d + f\rho(\omega))$ である．ゆえに，$N(d + f\omega) = ac$ より，$\alpha = d + f\rho(\omega)$ とおくと $\alpha\mathfrak{a} = a(\mathbf{Z}\alpha + \mathbf{Z}c) = a\mathfrak{b}$ となる．よって $\mathfrak{a}$ と $\mathfrak{b}$ は常に広義の意味で同値である．ゆえに (1) が証明された．

次に (2) を示す．まず $N(\epsilon) = -1$ となる元 $\epsilon \in \mathfrak{O}_f$ が存在すれば，$\epsilon\mathfrak{a} \subset \mathfrak{a}$ であるが，$\epsilon^{-1} = -\rho(\epsilon) \in \mathfrak{O}_f$ であるから $\epsilon^{-1}\mathfrak{a} \subset \mathfrak{a}$ でもあり，$\mathfrak{a} = \epsilon\mathfrak{a}$ である．よって $a^{-1}\alpha\epsilon\mathfrak{a} = \mathfrak{b}$ となり，$\mathfrak{a}$ と $\mathfrak{b}$ は狭義の意味で同値である．逆に，ある $\beta \in K^\times (N(\beta) > 0)$ について $\beta\mathfrak{a} = \mathfrak{b}$ とすると，$a^{-1}\alpha\beta^{-1}\mathfrak{a} = \mathfrak{a}$ である．ここで $\epsilon = a^{-1}\alpha\beta^{-1}$ とおくと，$N(\epsilon) < 0$ である．また $\epsilon\mathfrak{a} \subset \mathfrak{a}$ および $\mathfrak{a}$ が $\mathfrak{O}_f$ の固有イデアルであることより $\epsilon \in \mathfrak{O}_f$ である．同様に $\epsilon^{-1}\mathfrak{a} \subset \mathfrak{a}$ であるから，$\epsilon^{-1} \in \mathfrak{O}_f$ でもある．よって，$N(\epsilon), N(\epsilon^{-1})$ はともに整数であり，$N(\epsilon)N(\epsilon^{-1}) = N(1) = 1$ より，$N(\epsilon) = \pm 1$ であるが，$N(\epsilon) < 0$ であったから $N(\epsilon) = -1$ である．■

命題 6.13　K が実 2 次体とする．$\mathfrak{O}_f$ が元 ϵ で $N(\epsilon) = -1$ のものを含むときは狭義の類数と広義の類数は一致し，含まないときは狭義の類数は広義の類数の 2 倍である．

証明　ノルムが -1 の元を含めば広義の意味での同値関係 $\mathfrak{a} = \alpha\mathfrak{b}$ より，$\mathfrak{a} = \epsilon\alpha\mathfrak{b}$ がでるので，$N(\alpha) > 0$ または $N(\alpha\epsilon) > 0$ であり，狭義の意味でも同値になる．さてノルムが -1 の元を含まないときが問題で，この場合広義のイデアル類が 2 つの狭義のイデアル類に分かれることをいわねばならない．しかし，前の補題で見たように，このような ϵ が存在しないときには，任意の原始的な固有イデアルから，これと広義の意味では同値だが狭義の意味では同値でないイデアルがつくれたのであるから，これは証明された．■

通常の 2 次体論ではイデアル $\mathfrak{a}$ と $\alpha \in K^\times$ $(N(\alpha) < 0)$ に対して，いきなり $\alpha\mathfrak{a}$ をとって，これが $\mathfrak{a}$ と狭義の意味で同値か否かを見ることになる．通常のイデアル論では分数イデアルまで定義して乗法構造などを考えた上で理論を組み

立てるので，$\alpha\mathfrak{a}$ が $\mathfrak{O}_f$ の部分集合かどうかといった細かいことなどに注意を払う必要がないし，本来このほうが証明も理論もすっきりしている．しかし，なにぶん 2 次形式について触れた文献が少ないので，あえてやや迂遠な方法を用いてみた．

6.3　2 次形式の類数公式

この節では，まず原始的 2 次形式の類数（同値類の個数）の有限性を証明する．前節で述べたように，これは 2 次体の整環 $\mathfrak{O}_f$（極大整環とは限らない）の《狭義の》類数の有限性と同じことである．次に 2 次体の整環の広義の類数の公式を述べる．（証明は第 10 章まで延期する.） 前節で見たように狭義の類数は広義の類数がわかれば簡単に計算できる．実際は，極大整環の類数公式がわかれば，任意の整環の類数公式はそれに帰着させることができる．この帰着の様子は群論的に説明するのがわかりやすいが，第 10 章でゼータ関数を用いた別の証明を紹介する．

命題 6.14　与えられた判別式をもつ原始的 2 次形式の同値類の個数は有限である．特に判別式が f^2D_K の原始的 2 次形式の類数は有限である．

証明　判別式が平方数の場合は前に述べたので，判別式が f^2D_K (K は 2 次体，D_K は 2 次体の基本判別式) の場合を考えればよい．以下 f^2D_K を 1 つ固定し，2 次形式はすべてこれを判別式にもつもののみを考える．

まず，任意の原始的 2 次形式は $ax^2+bxy+cy^2$ で $|b|\le|a|\le|c|$ となるものに同値なことをいう．実際，まず同値な 2 次形式の中で，x^2 の係数 a について，$|a|$ が最も小さいものをとると，$(x,y)\to(-y,x)$ によって，x^2 の係数が c にかわることより，$|a|\le|c|$ がわかる．また，整数 $m\in\mathbf{Z}$ について，$(x,y)\to(x-my,y)$ として，

$$a(x-my)^2+b(x-my)y+cy^2=ax^2+(b-2am)xy+(c-bm+am^2)y^2$$

であるから，m を適当に選んで $-|a|\le b-2ma\le|a|$ とすることが可能である．よって，$|b|\le|a|\le|c|$ としてよい．（特に $D_K<0$ ならば正定値としているから $|b|\le a\le c$ である.） 一方，$b^2-4ac=f^2D_K$ より，

$$4|ac|-b^2\le|4ac-b^2|=f^2|D_K|$$

であるが，$b^2 \le a^2$, $a^2 \le |ac|$ より $3a^2 \le 4|ac| - b^2 \le f^2|D_K|$ であるから，$|a| \le \sqrt{f^2|D_K|/3}$. よって，$a$ は有限個しかない．よって，b も有限個であり，$c = (b^2 - f^2 D_K)/4a$ も有限個である．よって証明された． ∎

D_K を 2 次体の基本判別式として，$D = f^2 D_K$ とする．2 次体 $K = \mathbf{Q} + \mathbf{Q}\omega$ の整環 $\mathfrak{O}_f$ の広義の類数を $h(D)$ と書く．類数公式を記述するために，平方剰余記号を説明する．奇素数 p について mod p の平方剰余記号 $\left(\frac{a}{p}\right)$ が次で定義される．

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \notin p\mathbf{Z} \text{ で } x^2 \equiv a \bmod p \text{ となる整数 } x \text{ が存在する場合}, \\ -1 & a \notin p\mathbf{Z} \text{ で } x^2 \equiv a \bmod p \text{ となる整数 } x \text{ が存在しない場合}, \\ 0 & a \in p\mathbf{Z} \text{ の場合}. \end{cases}$$

平方剰余の相互法則として，次の 3 つの関係が知られている．

(1)　p, q を相異なる奇素数とすると

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}.$$

(2)　p を奇素数とすると

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}.$$

(3)　p を奇素数とすると

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

証明はここでは省略する．たとえば [33, 第 1 章] を参照されたい．

また，2 次体の判別式 D_K と素数 p について，$\chi_K(p)$ を

$$\chi_K(p) = \begin{cases} \left(\frac{D_K}{p}\right) & p \text{ が奇素数の場合}, \\ 1 & p = 2 \text{ で } D_K \equiv 1 \bmod 8 \text{ の場合}, \\ -1 & p = 2 \text{ で } D_K \equiv 5 \bmod 8 \text{ の場合}, \\ 0 & p = 2 \text{ で } D_K \equiv 0 \bmod 4 \text{ の場合} \end{cases}$$

とする．さらに，u が正の整数で $u = p_1^{e_1} \cdots p_r^{e_r}$ と素因数分解されるとき，$\chi_K(u) = \chi_K(p_1)^{e_1} \cdots \chi_K(p_r)^{e_r}$ とする．特に $\chi_K(1) = 1$ としている．実は，平

方剰余の相互法則などを用いると，$\chi_K(u)$ は $u \bmod D_K$ にしかよらないことが示され，これにより χ_K を $\mathbf{Z}$ 上の関数に拡張すると

$$\chi_K(-1) = \begin{cases} 1 & D_K > 0 \text{ の場合}, \\ -1 & D_K < 0 \text{ の場合} \end{cases}$$

となることが証明できるのであるが，詳しくは省略する ([94, §5] 参照)．このように拡張された χ_K は $|D_K|$ を法とする原始的指標となり，これを $\left(\frac{D_K}{u}\right)$ と書くことがある．本書でもしばしばこの記号によって上の指標 χ_K を表す．

さて，この $\chi_K(u) = \left(\frac{D_K}{u}\right)$ を用いて類数公式が記述できる．

定理 6.15

(1)　判別式 D_K の 2 次体 K の広義の類数は

$$h(D_K) = \begin{cases} -\dfrac{w}{|D_K|} \displaystyle\sum_{u=1}^{|D_K|-1} \left(\frac{D_K}{u}\right) u & D_K < 0 \text{ の場合}, \\ -\dfrac{1}{2\log(\varepsilon)} \displaystyle\sum_{u=1}^{D_K-1} \left(\frac{D_K}{u}\right) \log(\sin(u\pi/D_K)) & D_K > 0 \text{ の場合} \end{cases}$$

で与えられる．ただし，w は $\mathfrak{O}_{\max}$ に含まれる単数の個数の 2 分の 1, $D_K > 0$ のとき ε は K の基本単数を表す．

(2)　K の判別式 $D = f^2 D_K$ の整環 $\mathfrak{O}_f$ の類数は

$$h(D) = \frac{h(D_K)f}{[\mathfrak{O}_{\max}^{\times} : \mathfrak{O}_f^{\times}]} \prod_{p|f} (1 - \frac{1}{p}\left(\frac{D}{p}\right))$$

で与えられる．ここで環 R に対し，$R^{\times}$ は R の単数のなす群を表す．

前に述べたように，狭義の類数はこれからわかり，以上により原始的 2 次形式の類数もわかったことになる．類数公式の証明は，K が虚 2 次体のときは第 10 章で与える．実 2 次体のときは省略する．

虚 2 次体の類数はベルヌーイ数にきわめて近い量である．実際ここで $\chi(u) = \left(\frac{D_K}{u}\right)$ とおくと，4.2 節より

$$B_{1,\chi} = \frac{1}{|D_K|} \sum_{u=1}^{|D_K|-1} \chi(u) u \tag{6.3}$$

であるから，$D_K < 0$ ならば

$$h(D_K) = -wB_{1,\chi} \tag{6.4}$$

が成立する．

特に p が素数で，$p \equiv 3 \bmod 4$ かつ $p > 3$ ならば，$\mathbf{Q}(\sqrt{-p})$ の類数 $h(-p)$ は，(6.3) 式と平方剰余の相互法則を用いて，

$$h(-p) = -\frac{1}{p}\sum_{u=1}^{p-1}\left(\frac{u}{p}\right)u \tag{6.5}$$

とも書ける．

上の公式から $D = -3, -4, -7, -8, -11, -19, -43, -67, -163$ について $h(D) = 1$ であることがわかる．実は $h(D_K) = 1$ となる虚2次体（の判別式）はこれらに限ることが知られている．虚2次体の極大整環以外のものまで考えても，類数が1のものは，$D = -12, -16, -27, -28$ がふえるだけである．これにひきかえ，実2次体については類数1のものが無限に存在すると予想されている[3]が，証明は知られていない．

[3]ガウスの予想と呼ばれる．Gauss はその整数論の著書 *Disquisitiones Arithmeticae* [27] の 304 節において，基本単数の大きさとの関係など，的確な洞察を述べている．

第7章

ベルヌーイ数と虚2次体の類数との合同関係

この章では，虚2次体の類数とベルヌーイ数の間に成り立つ合同式（定理7.1）を証明する．その準備として，Hurwitz[1]が考察した“指数関数型整係数”（定義7.4）——われわれはこれを「フルビッツ整」と呼ぶことにする——級数について，必要なことを7.2節で述べる．これは定理7.1の証明のためだけならばどうしても必要というわけではないが，知っておくと何かと便利であると思われる．

7.1 類数とベルヌーイ数の合同式

$p > 3$ を $p \equiv 3 \mod 4$ なる素数とし，$h(-p)$ で判別式が $-p$ の虚2次体の類数を表す．このとき次の合同式が成り立つ[2]．

定理 7.1 p を上のとおりとするとき，

$$h(-p) \equiv -2B_{\frac{p+1}{2}} \mod p.$$

注意 7.2

（1） クラウゼン・フォンシュタウトの定理により，$B_{\frac{p+1}{2}}$ の分母は p と互いに素である．

（2） オイラーの公式 $\zeta(1-k) = -B_k/k$（72ページ定理5.4の（2））より

---

[1]Adolf Hurwitz (1859.3.26 ドイツ Hildesheim 生——1919.11.18 スイス Zürich 没)

[2]Augustin Louis Cauchy (1789.8.21 フランス Paris 生——1857.5.23 フランス Sceaux 没)による結果．ただし彼は左辺を，区間 $(0, p/2)$ における平方剰余，非剰余の個数の差で表しており，これが類数になることは Dirichlet の類数公式による．

$$\zeta(\frac{1-p}{2}) = -\frac{B_{\frac{p+1}{2}}}{\frac{p+1}{2}} \equiv -2B_{\frac{p+1}{2}} \mod p$$

であるので，定理はまた

$$h(-p) \equiv \zeta(\frac{1-p}{2}) \mod p$$

とも書ける．前章末の類数公式 (6.5) より特に

$$1 \leq h(-p) = \frac{1}{p}\left|\sum_{u=1}^{p-1}\left(\frac{u}{p}\right)u\right| \leq \frac{1}{p}\sum_{u=1}^{p-1} u = \frac{p-1}{2}$$

であるから，$h(-p)$ は mod p の値がわかると一意に決まる．したがって，上の合同式より，リーマンゼータ関数の負整数点での値 $\zeta(\frac{1-p}{2})$ が類数 $h(-p)$ を完全に「知っている」ことになる．

(3)　この定理の p 進モジュラー形式の言葉を用いた，より進んだ解釈については [72] を参照．

例 7.3　定理を使って類数を求めてみる．

(1)　$p = 7$ のとき，

$$-2B_{\frac{7+1}{2}} = -2B_4 = -2\left(-\frac{1}{30}\right) = \frac{1}{15} \equiv 1 \mod 7$$

より $h(-7) = 1$.

(2)　$p = 11$ のとき，

$$-2B_{\frac{11+1}{2}} = -2B_6 = -2\left(\frac{1}{42}\right) = -\frac{1}{21} = \frac{1}{1-22} \equiv 1 \mod 11$$

より $h(-11) = 1$.

(3)　$p = 19$ のとき，

$$-2B_{\frac{19+1}{2}} = -2B_{10} = -2\left(\frac{5}{66}\right) = -\frac{5}{33} = \frac{5}{5-38} \equiv 1 \mod 19$$

より $h(-19) = 1$.

(4)　$p = 23$ のとき，

$$-2B_{\frac{23+1}{2}} = -2B_{12} = -2\left(-\frac{691}{2730}\right) = \frac{691}{1365} \equiv \frac{1}{8} \equiv 3 \mod 23$$

より $h(-23) = 3$.

7.2 「フルヴィッツ整」級数

定義 7.4　有理数係数の形式的べき級数で，$\sum_{n=0}^{\infty} c_n \frac{t^n}{n!}$（$c_n$ はすべて整数）という形のもの全体の集合を $\mathcal{H}$ と書く．

$P(t) \in \mathcal{H}$ は $P(0), P'(0), P''(0), P^{(3)}(0), \cdots$ がすべて $\mathbf{Z}$ に入ることと同値である．たとえば $e^t, \log(1+t)$ などは $\mathcal{H}$ の元である．

命題 7.5

（1）　$\mathcal{H}$ は整域である．

（2）　$\mathcal{H}$ は（項別）微分 $\dfrac{d}{dt}$,（項別）積分 $\displaystyle\int_0^t$ で閉じている．

（3）　$\mathcal{H}$ の可逆元全体 $\mathcal{H}^{\times} = \{P(t) \in \mathcal{H} \mid P(0) = \pm 1\}$.

証明　(1)　$\mathcal{H}$ が積で閉じていることだけを確かめる（あとは自明）．$P(t) = \sum_{n=0}^{\infty} c_n \frac{t^n}{n!}$，$Q(t) = \sum_{n=0}^{\infty} d_n \frac{t^n}{n!}$ に対し，積 $P(t)Q(t)$ を $\sum_{n=0}^{\infty} e_n \frac{t^n}{n!}$ の形に書いたとき，係数 e_n は

$$e_n = \sum_{i=0}^{n} \binom{n}{i} c_i d_{n-i}$$

で与えられるので，c_i, d_{n-i} がすべて整数ならば e_n も整数である．

(2)　$P(t) = \sum_{n=0}^{\infty} c_n \frac{t^n}{n!} \in \mathcal{H}$ とすると，

$$P'(t) = \sum_{n=1}^{\infty} c_n \frac{t^{n-1}}{(n-1)!} = \sum_{n=0}^{\infty} c_{n+1} \frac{t^n}{n!},$$

$$\int_0^t P(t)dt = \sum_{n=0}^{\infty} c_n \frac{t^{n+1}}{(n+1)!} = \sum_{n=1}^{\infty} c_{n-1} \frac{t^n}{n!}$$

であるので，ともに $\mathcal{H}$ の元である．

(3)　$P(t) = \sum_{n=0}^{\infty} c_n \frac{t^n}{n!}$ が $\mathbf{Q}[[t]]$ において可逆であるために $c_0 \neq 0$ が必要である（14 ページ命題 1.9）．このとき，$\mathbf{Q}[[t]]$ での逆元 $P(t)^{-1}$ を $P(t)^{-1} = \sum_{n=0}^{\infty} b_n \frac{t^n}{n!}$ と書く．これが $\mathcal{H}$ に入るためには，$b_0 = c_0^{-1} \in \mathbf{Z}$ より，$c_0 = \pm 1$ が必要．他の各係数 b_n は $P(t)^{-1}$ の n 回微分 $\left(P(t)^{-1}\right)^{(n)}$ の定数項であるが，商の微分の公式によれば

$$\left(P(t)^{-1}\right)^{(n)} = \frac{P(t), P'(t), P''(t), \cdots \text{の整係数多項式}}{P(t)\,\text{のべき}}$$

の形であるから，$c_0 = P(0) = \pm 1$ であれば，$P(0), P'(0), P''(0), \cdots \in \mathbf{Z}$ より，この式の $t = 0$ での値は整数になる．したがって $P(t) \in \mathcal{H}^\times$．逆に $P(t) \in \mathcal{H}^\times$ ならば $P(t)^{-1}|_{t=0} = c_0^{-1} \in \mathbf{Z}$ より $c_0 = \pm 1$ である． ∎

注意 7.6　$\sin(t), \cos(t)$（関数 $\sin(x), \cos(x)$ の原点でのテイラー展開級数を $x = t$ として t の形式的べき級数と見たもの）はともに $\mathcal{H}$ の元であり，命題の (3) より $\cos(t) = 1 - t^2/2! + t^4/4! + \cdots$ は可逆元である．したがって $\tan(t) = \frac{\sin(t)}{\cos(t)}$ はフルヴィッツ整級数である．すなわち 22 ページ注意 1.18 の T_n（正接数）は整数である．

命題 7.7　$P(t) \in \mathcal{H}, P(0) = 0$ のとき，すべての $N \in \mathbf{N}$ に対して

$$\frac{P(t)^N}{N!} \in \mathcal{H}.$$

証明　帰納法による．$N = 1$ のときは自明．$N - 1$ まで成り立つとする．$\left(\frac{P(t)^N}{N!}\right)' = \frac{P(t)^{N-1}}{(N-1)!} P'(t)$ および $P(0) = 0$ より，

$$\frac{P(t)^N}{N!} = \int_0^t \frac{P(t)^{N-1}}{(N-1)!} P'(t) dt$$

であるが，帰納法の仮定と命題 7.5 (1),(2) より右辺は $\mathcal{H}$ の元となる． ∎

定義 7.8　$P(t)(\neq 0), Q(t) \in \mathcal{H}$ について，$\frac{Q(t)}{P(t)} \in \mathcal{H}$ なるとき，$P(t)|_H Q(t)$ または $Q(t) \equiv_H 0 \mod P(t)$ と書く．$Q_1(t) \equiv_H Q_2(t) \mod P(t)$ とは $P(t)|_H (Q_1(t) - Q_2(t))$ のこととする．

特に，m を整数とするとき（これも $\mathcal{H}$ の元である），$Q_1(t) \equiv_H Q_2(t) \mod m$ とは，$Q_1(t) = \sum_{n=0}^{\infty} c_n^{(1)} \frac{t^n}{n!}$，$Q_2(t) = \sum_{n=0}^{\infty} c_n^{(2)} \frac{t^n}{n!}$ と書くとき，$c_n^{(1)} \equiv c_n^{(2)} \mod m$ がすべての n について成り立つことにほかならない．

7.3　定理 7.1 の証明

$\frac{p-1}{2} = m$ とおく．$p > 3$ より $m > 1$ である．94 ページの類数公式 (6.5)

$$h(-p) = -\frac{1}{p} \sum_{u=1}^{p-1} \left(\frac{u}{p}\right) u$$

において，和を $u < p/2$ と $u > p/2$ に分けて，$p \equiv 3 \mod 4$ より $\left(\frac{-1}{p}\right) = -1$

に注意すると，

$$ph(-p) = -\sum_{0<u<p/2}\left(\frac{u}{p}\right)u - \sum_{0<u<p/2}\left(\frac{p-u}{p}\right)(p-u)$$
$$= -2\sum_{0<u<p/2}\left(\frac{u}{p}\right)u + p\sum_{0<u<p/2}\left(\frac{u}{p}\right). \tag{7.1}$$

一方，u の偶奇で分けると，

$$ph(-p) = -\sum_{0<u<p/2}\left(\frac{2u}{p}\right)(2u) - \sum_{0<u<p/2}\left(\frac{p-2u}{p}\right)(p-2u)$$
$$= -4\sum_{0<u<p/2}\left(\frac{2u}{p}\right)u + p\sum_{0<u<p/2}\left(\frac{2u}{p}\right).$$

これより

$$\left(\frac{2}{p}\right)ph(-p) = -4\sum_{0<u<p/2}\left(\frac{u}{p}\right)u + p\sum_{0<u<p/2}\left(\frac{u}{p}\right). \tag{7.2}$$

(7.1) 式の 2 倍から (7.2) 式を引くと

$$\left(2-\left(\frac{2}{p}\right)\right)ph(-p) = p\sum_{0<u<p/2}\left(\frac{u}{p}\right),$$

すなわち

$$h(-p) = \frac{1}{2-\left(\frac{2}{p}\right)}\sum_{a=1}^{m}\left(\frac{a}{p}\right)$$

が得られた．これといわゆるオイラーの基準 $\left(\frac{a}{p}\right) \equiv a^m \mod p$（[33, 定理 1.9] 参照）より

$$h(-p) \equiv \frac{1}{2-2^m}\sum_{a=1}^{m} a^m \mod p.$$

したがって，定理 $h(-p) \equiv -2B_{m+1} \mod p$ を証明するには，

$$\sum_{a=1}^{m} a^m \equiv -2(2-2^m)B_{m+1} \mod p$$

を証明すればよいことになる．さらに $2 \equiv \frac{1}{m+1} \mod p$ および $-(2-2^m) \equiv -(2^{2m+1}-2^m) \equiv 2^m(1-2^{m+1}) \mod p$ により変形して，

$$\sum_{a=1}^{m} a^m \equiv 2^m(1-2^{m+1})\frac{B_{m+1}}{m+1} \mod p$$

を証明する．

まず，$\frac{t}{e^t-1} = 1 - \frac{t}{2} + \sum_{n=2}^{\infty} B_n \frac{t^n}{n!}$ より

$$\begin{aligned}
\frac{1}{e^t+1} &= \frac{1}{e^t-1} - \frac{2}{e^{2t}-1} \\
&= \frac{1}{t}\left(\left(1 - \frac{t}{2} + \sum_{n=2}^{\infty} B_n \frac{t^n}{n!}\right) - \left(1 - \frac{2t}{2} + \sum_{n=2}^{\infty} B_n \frac{(2t)^n}{n!}\right)\right) \\
&= \frac{1}{2} + \sum_{n=2}^{\infty} (1-2^n) B_n \frac{t^{n-1}}{n!} \\
&= \frac{1}{2} + \sum_{n=1}^{\infty} (1-2^{n+1}) \frac{B_{n+1}}{n+1} \cdot \frac{t^n}{n!}.
\end{aligned}$$

ここで $t \mapsto 2t$ として両辺を 2 倍すると

$$\frac{2}{e^{2t}+1} = 1 + \sum_{n=1}^{\infty} 2^{n+1}(1-2^{n+1}) \frac{B_{n+1}}{n+1} \frac{t^n}{n!}. \tag{7.3}$$

さて，

$$\begin{aligned}
\frac{2}{e^{2t}+1} &= \frac{1}{1-\frac{1-e^{2t}}{2}} \\
&= 1 + \left(\frac{1-e^{2t}}{2}\right) + \left(\frac{1-e^{2t}}{2}\right)^2 + \left(\frac{1-e^{2t}}{2}\right)^3 + \cdots
\end{aligned}$$

であり，$\left(\frac{1-e^{2t}}{2}\right) = -\sum_{n=1}^{\infty} 2^{n-1} \frac{t^n}{n!} \in \mathcal{H}$ なので，$\frac{2}{e^{2t}+1} \in \mathcal{H}$. また命題 7.7 より $\left(\frac{1-e^{2t}}{2}\right)^N \equiv_H 0 \mod N!$. 特に，$N \geq 2$ ならば $\left(\frac{1-e^{2t}}{2}\right)^N \equiv_H 0 \mod 2$ である．これと，$\frac{1-e^{2t}}{2}$ の $\frac{t^n}{n!}$ の係数は $n \geq 2$ ならば 2 で割れていることから，

$$\frac{2}{e^{2t}+1} \equiv_H 1 + t \mod 2.$$

よって (7.3) 式より，$n \geq 2$ のとき

$$2^n(1-2^{n+1}) \frac{B_{n+1}}{n+1} \in \mathbf{Z}$$

を得る．次に，

$$\begin{aligned}(1+e^{2t})\sum_{a=0}^{m} e^{4at} &= \sum_{a=0}^{m}\left(e^{4at}+e^{(4a+2)t}\right)=\sum_{j=0}^{2m+1} e^{2jt}\\ &= \sum_{j=0}^{p}\sum_{n=0}^{\infty}\frac{(2jt)^n}{n!}\\ &= \sum_{n=0}^{\infty}\left(\sum_{j=0}^{p}(2j)^n\right)\frac{t^n}{n!}\\ &= p+1+\sum_{n=1}^{\infty}2^n\left(\sum_{j=1}^{p}j^n\right)\frac{t^n}{n!}\\ &\equiv_H 1-\sum_{\substack{n\geq 1\\ p-1|n}} 2^n\frac{t^n}{n!} \mod p.\end{aligned}$$

（ここで，40 ページの (3.1) 式，つまり $p-1|n$ ならば $\sum_{j=1}^{p} j^n \equiv -1 \bmod p$, さもなくば $\sum_{j=1}^{p} j^n \equiv 0 \bmod p$ を使った.） この両辺に $\frac{2}{e^{2t}+1}$ $(\in \mathcal{H})$ をかけると,

$$2\sum_{a=0}^{m} e^{4at} \equiv_H \frac{2}{e^{2t}+1}\left(1-\sum_{\substack{n\geq 1\\ p-1|n}} 2^n\frac{t^n}{n!}\right) \mod p.$$

両辺の $\frac{t^m}{m!}$ の係数を比べると（$m=\frac{p-1}{2}<p-1$ に注意），(7.3) 式より

$$2\sum_{a=0}^{m}(4a)^m \equiv 2^{m+1}(1-2^{m+1})\frac{B_{m+1}}{m+1} \mod p.$$

両辺を 2 で割り，$4^m = 2^{p-1} \equiv 1 \mod p$ を使うと

$$\sum_{a=0}^{m} a^m \equiv 2^m(1-2^{m+1})\frac{B_{m+1}}{m+1} \mod p.$$

これがすなわち証明しようとしていた式であった. ∎

第 8 章

指数和とベルヌーイ数

ベルヌーイ数と 1 のべき根に関する算術的な等式について少し解説したい．つまり，いくつか公式集のようなものを解説しようと思う．そうはいっても，これから述べる「公式」は公式集というには種類も少ないし，ずいぶんとやさしいものも含まれている．しかしどこかの本にでているものの引き写しというようなものではない．（実際には，そもそもそういう本は存在しないように思う．文献 [13] などがムードとしては近いかもしれないが，実際に扱っている内容はまったく違う.） この節の内容は著者自身が折に触れ必要があって証明した備忘録のようなものである．このような内容のみを専門にする研究者が存在するとはとても思えないので，ある意味で全員アマチュアであって，誰でも新しい何かの公式を発見するチャンスがあるという意味では，大げさにいえば万人に開かれた数学ともいえるかもしれない．経験してみないとわからないことも多いようなので，何かで突然必要になったときの参考にでもなれば幸いである．

さて，数学辞典や数学公式集を見ると，昔から知られている特殊関数の公式というものがたくさん掲載されている．ある関数と他の関数の間の関係式がいろいろ成り立つというものである．公式とはいっても，これらは要するに等式なのだから，等しくなるようにあたりまえの変形を何度も繰り返して計算するといろいろ公式が得られるのは当然であろうと思うかもしれないが，さにあらず，だてに公式という名前がついているわけではない．甘く見て実際に自分で公式集の関係式を証明してみようと思ったりすると，意外の難しさに辟易することがある．ここには先人に学ばなければ到底わからないような数学世界の蓄

積があるように思う．さらには，こういう関係式は，何かを計算するという観点から見てみると一見，左辺と右辺のどちらが答と思いたいのか，はたまた変形の結果単純になったのか，かえって複雑になったのか，また要するにどういう意味なのかよくわからないことも多い．もちろん具体的な物事の解釈が 1 通りしかないなどということはあり得ないから，解釈は各人各様ということにもなる．

さて，こういう古典的な物理学などに登場する特殊関数とは非常に異なるが，これから解説する指数和（1 のべき乗根や指標に関する和）はそのムードはかなり特殊関数に似ている．たとえば，問題が 1 つひとつわりと散発的で決まった計算法というものがない．でたらめに式を書いたらいつ答が綺麗になるのかはもちろんわからない．またたとえ答が綺麗だということが数値例などから確信でき，答の形が予想できる場合でさえ，実際に予想どおりになっていることを証明するのは，何のアイデアも思いつかない場合には非常に難しく思える．さらには，いろいろ複雑な考察の結果，答が得られたとしても，たまたま得られた証明はあまりスマートではないかもしれず，少し手法をかえればまったく単純な証明が得られたりもする．しかし，証明が得られるまでは，そもそも証明がやさしいのか難しいのかさえ見当がつかない．あるいはいろいろな式変形が可能であるが，変形の結果やさしくなるのか難しくなるのかよくわからない，などなど．

ここでは 1 つの観点として，指数和を一般ベルヌーイ数で表せたら答として満足するということにしよう．実はこのような指数和とベルヌーイ数の関係は，昔から保型形式の次元公式などの中にときどき現れている．ここで保型形式の正確な説明はできないが，つまり，整数論で大切な，保型形式と呼ばれるある種の不変性をもつ関数のなす有限次元ベクトル空間があって，そのベクトル空間の次元を計算したいというわけである．この次元の計算法は大雑把にいって跡公式とリーマン・ロッホの定理という 2 種類のまったく異なる方法があって，通常は，非常に複雑な延々たる計算の結果，次元の公式が得られるのだが，次元を 2 通りの異なる方法で別々に計算すると，でてくる答（次元）の見かけ上の表示が異なることがある．きわめて単純化していえば一方が指数和で一方がベルヌーイ数のことがある．しかしもともと同じ次元を違う方法で計算しただ

けなのだから，両者は等しいはずで，よって指数和とベルヌーイ数との関係式が得られるというわけである．関係式が得られるには違いないが，関係式という観点からは，この証明はきわめて遠回りである．当然単純な初等的な証明がないかと思うものである．しかしときとして，これは難しい．実際，現在でも初等的な証明の知られていない関係式などがある．1 つ複雑な例をあげてみよう．p を $p \equiv 3 \bmod 4$ となる素数とする．$\zeta = e^{2\pi i/p}$ とおく．すると次の公式

$$\sum_{(a,b,c)\in S} \frac{\psi(abc)}{(1-\zeta^a)(1-\zeta^b)(1-\zeta^c)} = -\sqrt{-p}\left(\frac{p+1}{4}B_{1,\psi} + \frac{1}{6}B_{3,\psi}\right)$$

が成り立つ．（ここで $S = \left\{(a,b,c) \in (\mathbf{F}_p^\times)^3; ab+bc+ca=0\right\}$，$\mathbf{F}_p$ は標数 p の素体 $\mathbf{Z}/p\mathbf{Z}$，ψ は平方剰余指標，$B_{n,\psi}$ は一般ベルヌーイ数.） この関係式は次元公式を契機として [61] で予想され，[40] で証明された．これは前に述べたような遠回りな証明である．したがって，この指数和の公式の証明をここに書くにはあまりに長く複雑すぎて無理である．ここで，もっと初等的な直接証明がないかどうか知りたくなるのは人情である．しかしこのような初等的な別証は 2000 年 12 月現在では知られていない．前にも述べたように，初等的な直接証明があるとしても，得られてみないうちは直接証明が単純なのか複雑なのか見当もつかない．

以下で述べるのはこれに比べると，はるかにやさしい和である．しかし，やさしいというのはあくまで結果論であって，知らないと数学の研究者でも時としてつまずくという点では特殊関数にも似ているであろう．

8.1 最も簡単な例

すぐに説明できる，なるべく簡単な問題例をあげて具体的な解説を行ってみよう．素数 p について，$\zeta_p = e^{2\pi i/p}$ とおく．（これはもちろん p 乗すると 1 になる複素数のうち特別なものである.） たとえば和 $\sum_{a=1}^{p-1} \frac{1}{1-\zeta_p^a}$ を考えよう．この和は実は

$$\sum_{a=1}^{p-1} \frac{1}{1-\zeta_p^a} = \frac{p-1}{2} \tag{8.1}$$

となる．さらに $1/(1-\zeta_p^a)$ の分子に a の平方剰余記号や指標をつけ加えた類似

の和はベルヌーイ数やガウス和で記述できる．このように1のべき乗根と指標などを組み合わせてつくった和を漠然と指数和とか指標和とか呼んでいる．

最初にあげた例 (8.1) については，計算は非常に簡単である．また指標等をつけた類似の和についても，この種の公式を計算するのはそれほど難しくはない．しかしその計算法を具体的に解説した本は筆者の知る限りほとんどない．また実際上，必ず計算できる方法があるわけでもない．計算するといっても，答もまた式なのであるから，どういう式を得たら，答として満足した気分になるのかということは当然の疑問である．ここでは一般ベルヌーイ数や p などの単純な多項式で答が得られればそれで満足することにする．

証明 0　一番簡単な証明を述べる．ζ_p^a $(1 \leq a \leq p-1)$ は $X^p - 1 = 0$ の1以外の相異なる $p-1$ 個の根であるから

$$\frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + 1 = \prod_{a=1}^{p-1}(X - \zeta_p^a)$$

である．両辺の対数をとって微分したものを比較する．すなわち左辺は

$$\frac{d}{dX}\log(X^{p-1} + X^{p-2} + \cdots + 1) = \frac{\sum_{a=1}^{p-1} aX^{a-1}}{X^{p-1} + \cdots + 1}$$

であり，右辺は

$$\frac{d}{dX}\sum_{a=1}^{p-1}\log(X - \zeta_p^a) = \sum_{a=1}^{p-1}\frac{1}{X - \zeta_p^a}$$

である．ここで $X = 1$ とすれば，$p^{-1}\sum_{a=1}^{p-1} a = (p-1)/2$ より証明すべき関係式が得られた．　■

証明 1　次に述べる証明は，初等的な代数学を勉強するとでてきそうな証明である．少し代数学の道具（円分体のガロア理論）を使うから，道具を全然知らないとよく理解できない．しかし実はこの問題に関してはこの解答は非常によい方法とは言い難いところがある．全然述べないと手法が一面的になりすぎるように思うので解説を書くが，後から使うわけではないから，道具をあまり知らない読者は，ここはスキップして次の証明2を読むことをお勧めする．

1のべき乗根，すなわち何乗かすると1になる複素数については，Gauss の時代からよく調べられている．複素平面上に1の n 乗根をすべて図示すれば，半径1の円の周を n 等分する点の集まりになる．つまりこれはちょうど正 n 角

形の頂点全部を与えている．有理数体上 1 の n 乗根で生成される体のことを円分体というのはそのためである．Gauss は円分体について，深く研究した（[27, 第 7 章]）．たとえばその 1 つのわかりやすい応用として正十七角形は定規とコンパスで作図できることを示した．これは円分体の部分体にどのようなものがあるかを調べて得られる結果である．

さて，われわれの問題を解く 1 つの方法は，いわば円分体論（というか一般の体論）の応用問題と見なしてしまう方法である．ここでは少し円分体のガロア理論の知識を仮定する．円分体 $\mathbf{Q}(\zeta_p)$ は $\mathbf{Q}$ 上のガロア拡大であり，$1 \leq a \leq p-1$ について，$\zeta_p \mapsto \zeta_p^a$ なる写像 σ_a の全体が円分体 $\mathbf{Q}(\zeta_p)$ の $\mathbf{Q}$ 上のガロア群を与える．よって，(8.1) 式に現れる和は $\mathbf{Q}(\zeta_p)$ の元 $x = 1/(1-\zeta_p)$ の $\mathbf{Q}$ 上のトレース（$\mathbf{Q}(\zeta_p)$ のある 1 つの元 x にガロア群の元 σ_a を作用させたものすべての和 $\sum_{a=1}^{p-1} \sigma_a(x)$）である．これはガロア群の各元 σ_a で不変であるから，ガロア理論の一般論より，有理数になる．$\mathbf{Q}(\zeta_p)$ の $\mathbf{Q}$ 上の拡大次数（すなわち $\mathbf{Q}$ 上のベクトル空間としての次元）は $p-1$ であるが，$\zeta_p = 1 - 1/x$ より，x 自身も $\mathbf{Q}(\zeta_p)$ を生成するから，x の $\mathbf{Q}$ 上の最小多項式も $p-1$ 次である．ζ_p の最小多項式は $1 + X + X^2 + \cdots + X^{p-1} = (X^p - 1)/(X-1)$ だから，$-1/x = \zeta_p - 1$ の最小多項式は $((X+1)^p - 1)/X$ である．$X = -1/Y$ とすれば，これは $-Y^{1-p}((Y-1)^p - Y^p)$ と書き換えられるから，x の，最高次の係数が 1 となる最小多項式は

$$\frac{1}{p}(Y^p - (Y-1)^p)$$

である．x のトレースはこの多項式の Y^{p-2} の係数 $\times(-1)$ であるから 2 項定理より，

$$\frac{1}{p} \times \frac{p(p-1)}{2} = \frac{p-1}{2}$$

となる．よって (8.1) 式を得る． ∎

証明 2　証明 1 はいかにも武骨であるし，意外に応用が利かない．ここでもっと一般的な手法を述べよう．いま t を不定元（考えている体上超越的な元という意味．変数と思えばよい）として，有理式

$$\frac{1}{1-\zeta_p t}$$

を考える．これを形式的べき級数として展開して計算すると

$$\frac{1}{1-\zeta_p t} = \sum_{i=0}^{\infty} \zeta_p^i t^i = \sum_{j=0}^{\infty}\sum_{c=0}^{p-1} \zeta_p^c t^{c+pj} = \frac{\sum_{c=0}^{p-1} \zeta_p^c t^c}{1-t^p}$$

となる．以上は $|t| < 1$ ならば収束べき級数としても正しい．よってここで，$t \to 1$ とすると，たとえば微分の定義（あるいはロピタル[1]の定理）などにより，容易に

$$\frac{1}{1-\zeta_p} = -\frac{1}{p}\sum_{c=1}^{p-1} c\zeta_p^c$$

となる．以上の計算では $\zeta_p^p = 1$ かつ $\zeta_p \neq 1$ という性質しか用いていないから，a が p と素なとき ζ_p を ζ_p^a にかえて同様の計算をしてもよく，

$$\frac{1}{1-\zeta_p^a} = -\frac{1}{p}\sum_{c=1}^{p-1} c\zeta_p^{ac}$$

が得られる．ここで a について和をとると，

$$\sum_{a=1}^{p-1} \zeta_p^{ca} = \sum_{a=0}^{p-1} \zeta_p^{ca} - 1 = \begin{cases} -1 & c \not\equiv 0 \bmod p \text{ のとき}, \\ p-1 & c \equiv 0 \bmod p \text{ のとき} \end{cases}$$

より

$$\sum_{a=1}^{p-1} \frac{1}{1-\zeta_p^a} = -\frac{1}{p}\sum_{c=1}^{p-1}(-c) = \frac{1}{p} \times \frac{p(p-1)}{2} = \frac{p-1}{2}$$

となり，(1) が得られた．　■

証明 2 のほうがあまり特別な方針なしに，いわば発見的に形式的に計算できる点でわかりやすいと思われる．（実は上ででてきた $(1-\zeta^a)^{-1}$ を表示する式は，補題 8.5 で見るように，よく考えればもっと単純に証明できる．しかし上で与えた証明は結論を予想しなくても計算が機械的に続行できるという点では面白いと思う．）

ちなみに，円分体 $\mathbf{Q}(\zeta_p)$ は $\mathbf{Q}$ 上 $p-1$ 次のベクトル空間であるが，その基底

---

[1] Guillaume François Antoine de l'Hôpital（1661 フランス Paris 生——1704.2.2 フランス Paris 没）

として $1, \zeta_p, \cdots, \zeta_p^{p-2}$（または $\zeta_p, \cdots, \zeta_p^{p-1}$ など）がとれるので，$\mathbf{Q}(\zeta_p)$ の元 $(1-\zeta^a)^{-1}$ がこれらの有理数係数の線形結合で表せるのは当然である．原理的には，どのような体についても，与えられた元の逆数を基底で表示する方法はある．しかしこのような線形結合の具体的な表示がいつでも単純に求まるかどうかはわからない．いまはたまたまこのような表示が単純だったのでこれを使用することができた．

8.2 ガウス和

指数和と一般ベルヌーイ数の関係の説明に入る前に，ガウス和について説明する．ガウス和の一番単純な定義は，素数 p に対して

$$g(p) = \sum_{x=0}^{p-1} \zeta_p^{x^2}, \qquad \zeta_p = e^{\frac{2\pi i}{p}}$$

で与えられる．この量は Gauss により計算されているが，結論は大変綺麗である．すなわち，

$$g(p) = \sqrt{(-1)^{(p-1)/2}p}$$

である．ここで平方根の取り方は，$p \equiv 1 \bmod 4$ ならば $\sqrt{p}$ はもちろん正のものをとり，$p \equiv 3 \bmod 4$ ならば $\sqrt{-p}$ は偏角が $\pi/2$ のものをとるのである．以下に見るように $g(p)^2 = (-1)^{(p-1)/2}p$ であることを証明するのは非常に簡単だが，これの平方根である $g(p)$ の符号を決めるのはかなり難しい．Gauss は証明を得るのに実に 4 年の期日を費やしたそうである[2]．現在ではこの符号を決定す

[2]Gauss は Olbers に宛てた 1805 年 9 月 3 日付の手紙（全集 Xp.24）にこう書いている．「……ここ 4 年間，この難題を解こうとしてあれやこれやと空しい試みをしなかった週はほとんどありませんし，最近はまた特に精魂を注いでいました．ですが考えることのすべて，やってみることのことごとくは徒労に終わり，いつもがっかりしてペンを置かなければならないのでした．それがついに数日前，うまく行ったのです．これはしかし私の難儀な探求によるものではなく，ただ神の恵みによってできた，と言いたい思いです．雷が落ちるように，謎は解けたのです．……とても奇妙なのですが，この解答もいまや，この数年ほど多くの日々を費やしてもいない，他の多くのことよりも，やさしく思えるのです．いつかこれについて講義をしても，きっと誰も，私が陥っていた長い窮地になど気づきもしないだろうと思います.」ちなみに，Olbers (Heinrich Wilhelm Matthias Olbers, 1758—1840) は医者で天文学者．Gauss を一躍有名にさせた最大の小惑星ケレス (Ceres) ——1801 年元日にイタリアの天文学者 Giuseppe Piazzi (1746—1826) により発見されるも観測の困難から行方不明，その

る方法は数多く知られているが，これを掲載するのは本書の流れからするとやや異質な感じがしないでもない．よって，符号の決定については他書にゆずる．(たとえば [13] には数多くの証明が紹介されている．)

さて，このガウス和を考えるのに，少し別の表示方法もある．いま ψ で，92 ページで定義した mod p の平方剰余記号を表すとし（$\psi(n)=\left(\frac{n}{p}\right)$），

$$g(\psi)=\sum_{n=0}^{p-1}\psi(n)\zeta_p^n$$

とする．各 n に対し $n\equiv x^2 \bmod p$ となる $x\in\mathbf{Z}$ の $\bmod p$ での代表の個数は $1+\psi(n)$ で与えられるから，

$$g(p)=\sum_{n=0}^{p-1}(1+\psi(n))\zeta_p^n=\sum_{n=0}^{p-1}\zeta_p^n+\sum_{n=0}^{p-1}\psi(n)\zeta_p^n.$$

ここで最初の和は明らかに 0 であるから，これは $g(\psi)$ に一致する．

ここでは以下で必要になるもっと一般のガウス和について説明したい．上記のガウス和の定義で，x^2 を一般の 2 次形式とベクトルに取り替えて定義すると「2 次形式のガウス和」が定義される．これはテータ関数の変換公式などで重要な役割を演ずるが，ガウスの公式のように計算可能な量である．一方で，ψ を一般のディリクレ指標にすれば，指標に付随するガウスの和が定義される．本書で取り扱うのはこちらの場合である．

定義 8.1　χ を f を導手とする原始的ディリクレ指標とし，$\zeta_f=e^{2\pi i/f}$ とおく．

$$g(\chi)=\sum_{n=0}^{f-1}\chi(n)\zeta_f^n$$

とおき，これを指標 χ に付随するガウス和という．

一般にも $g(\chi)$ の絶対値は簡単な量であり $g(\chi)\overline{g(\chi)}=f$ となる．（証明はあとで述べる．）しかし χ が一般の場合はガウスの和をこれ以上具体的に書く公式は存在しない．$\chi^2=1$ のときには公式が存在するが，これはあとで述べる．

補題 8.2　χ を f を導手とする原始的ディリクレ指標とし，a を任意の整数

位置を Gauss は計算によりつきとめた——を 1802 年の元日に再発見したのは Olbers である．また，1802 年に小惑星パラス (Pallas)，1807 年にベスタ (Vesta) を新しく発見している．Gauss が，友人の中で最も頻繁に訪れたのが Olbers であったという．

とするとき，

$$\overline{\chi(a)}g(\chi) = \sum_{n=1}^{f} \chi(n)\zeta_f^{an}$$

が成り立つ．特に $\overline{g(\chi)} = \chi(-1)g(\overline{\chi})$ である．

この関係式のポイントは a が f と素でなくても成り立つ点にあり，指数和の計算で，しばしば有用である．すなわち，この式は，a が f と素であれば，an をあらたに n と置き換えて明らかであるが，素でなくても，実は両辺が 0 になるので成り立つのである．

補題の証明 a が f と素でなければディリクレ指標の定義より，もちろん左辺は 0 であるが，このとき右辺も 0 である．なぜなら，$(a,f) = d > 1$ とするとき，ζ_f^{an} は $n \bmod f/d$ にしかよらないが，$1 \le n \le f$ で $1 \bmod f/d$ なるものは，$(\mathbf{Z}/f\mathbf{Z})^\times$ の中で群をなし，したがって f と素な任意の固定された n_0 に対して，

$$\sum_{n\equiv n_0 \bmod f/d} \overline{\chi(n)} = \overline{\chi(n_0)} \sum_{n\equiv 1 \bmod f/d} \overline{\chi(n)} = 0$$

だからである．

$a = -1$ として両辺の共役をとれば $\overline{g(\chi)} = \chi(-1)g(\overline{\chi})$ が得られる． ■

ガウス和は 0 にはならないから，上の式は

$$\chi(a) = g(\overline{\chi})^{-1} \sum_{n=1}^{f} \overline{\chi(n)}\zeta_f^{an} \tag{8.2}$$

と書き換えておいてもよい．

補題 8.3 次が成り立つ．

$$g(\chi)\overline{g(\chi)} = f.$$

証明 補題 8.2 により，任意の整数 a に対して

$$\chi(a)\overline{\chi(a)}g(\chi)\overline{g(\chi)} = \sum_{n,m=1}^{f-1} \chi(n)\overline{\chi(m)}\zeta_f^{a(n-m)}.$$

この両辺の $a = 0,\cdots,f-1$ にわたる和をとると，左辺は，$(a,f) = 1$ ならば $\chi(a)\overline{\chi(a)} = 1$，それ以外は 0 であるから $\varphi(f)g(\chi)\overline{g(\chi)}$ となる．ここで $\varphi(f)$ はオイラー関数，つまり 1 から f までの自然数の中で f と素なものの個数である．右辺は，

$$\sum_{a=0}^{f-1} \zeta_f^{a(n-m)} = \begin{cases} 0 & n \neq m \text{ の場合}, \\ f & n = m \text{ の場合} \end{cases}$$

を用いて，

$$f \times \sum_{n=1}^{f-1} \chi(n)\overline{\chi(n)} = f\varphi(f)$$

になる．両者を比較して，補題を得る． ∎

次に $\chi^2 = 1$ の原始的ディリクレ指標に対するガウス和の公式を説明しておこう．

命題 8.4　χ を単位指標以外の $\chi^2 = 1$ となる原始的ディリクレ指標とすると，χ はある 2 次体 K とその判別式 D_K によって $\chi(u) = \chi_K(u) = \left(\frac{D_K}{u}\right)$ と書ける．また，このとき

$$g(\chi_K) = \sqrt{D_K}$$

である．

証明は中国の剰余定理により各素数べきに分解して，素数のときのガウス和の公式に帰着すればよい．この証明の途中で平方剰余の相互法則などが必要であるが，詳しくは省略する．[13] などを参照のこと．

8.3　指数和と一般ベルヌーイ数

この節では 2 つ前の節と同じような和を指標つきで考える．実はこちらのほうが遥かに面白くなる．前節では 1 の素数乗根の場合だけ述べたが，この節ではもっと一般に 1 の f 乗根 $\zeta_f = e^{2\pi i/f}$ で考える．いちいち f を添え字につけるのも煩わしいので，今後自然数 f をずっと固定しておいて，ζ_f を単に ζ と書くことにする．以下では前節のような和を，一般ベルヌーイ数と簡単な組み合わせ的な数で記述する公式を求める方法を述べる．

まず，a が f で割り切れないとき，次のような公式が得られる．（この公式は第 11 章 11.2 節でも利用される.）

補題 8.5　$f \nmid a$ とすると

$$\frac{1}{1-\zeta^a} = -\frac{1}{f}\sum_{c=1}^{f-1} c\zeta^{ac}.$$

証明 前節の証明 2 とまったく同じ計算をすればよいが，ここではもっと直接的な証明を与えておく．多項式の計算により

$$\begin{aligned}(1-X) \times \sum_{c=1}^{f-1} cX^c &= \sum_{c=1}^{f-1}(c-(c-1))X^c - (f-1)X^f \\ &= \sum_{c=1}^{f} X^c - fX^f\end{aligned}$$

である．ここで $X = \zeta^a$ を代入すると，

$$\sum_{c=1}^{f} \zeta^{ac} = \frac{\zeta^a(1-\zeta^{af})}{1-\zeta^a} = 0$$

より，

$$(1-\zeta^a)\sum_{c=1}^{f-1} c\zeta^{ac} = -f\zeta^{af} = -f$$

である．よって両辺を $-f(1-\zeta^a)$ で割って，補題の関係式を得る． ∎

さて，導手が f のディリクレ指標（f を法とする原始的なディリクレ指標）χ を考える．まず

$$P_k(\chi) = \sum_{a=1}^{f} \frac{\chi(a)}{(1-\zeta^a)^k}$$

とおいて，これを記述することを考えよう．もちろん $f = 1$ ならば，このような形の分母はいつでも零になって意味がないので，以下では $f > 1$ と仮定する．前の節のとおり，χ に関するガウス和を

$$g(\chi) = \sum_{a=1}^{f} \chi(a)\zeta^a$$

と定義する．指数の和を少々一般的に取り扱うために

$$P_{k,\chi}(t) = \sum_{a=1}^{f} \frac{\chi(a)}{(1-\zeta^a e^t)^k}$$

とおく．$P_{k,\chi}(0) = P_k(\chi)$ である．次が成り立つ．

$$P_{1,\chi}(0) = -g(\chi)B_{1,\overline{\chi}}. \tag{8.3}$$

証明 前の補題と補題 8.2 より

$$P_{1,\chi}(0) = -\frac{1}{f}\sum_{a=1}^{f}\chi(a)\sum_{c=1}^{f-1}c\zeta^{ac} = -\frac{1}{f}g(\chi)\sum_{c=1}^{f}\overline{\chi(c)}c = -g(\chi)B_{1,\overline{\chi}}$$

である．最後の等式は 4.2 節にあげた $B_{1,\chi}$ の式 (4.1)（54 ページ）を用いた．∎

実は $P_{1,\chi}(t)$ はほとんど一般ベルヌーイ数の定義式そのものである．実際，展開して計算してみれば

$$P_{1,\chi}(t) = \sum_{a=1}^{f}\sum_{j=0}^{\infty}\chi(a)\zeta^{aj}e^{jt} = g(\chi)\sum_{j=0}^{\infty}\overline{\chi(j)}e^{jt} = -g(\chi)\frac{\sum_{j=0}^{f-1}\overline{\chi(j)}e^{jt}}{e^{ft}-1}$$

である．（ここで e^t 自身を形式的に変数と見なして，形式的べき級数として展開している．ないしは $t=-\infty$ の近傍で展開しているといってもよい．いずれにせよ最終的には e^t の有理関数どうしの等式であり，どの意味であれ，計算は正当なものである.）いま $f>1$ としているので，$\chi(0)=\chi(f)=0$ より，定義によって

$$P_{1,\chi}(t) = -g(\chi)\sum_{n=1}^{\infty}B_{n,\overline{\chi}}\frac{t^{n-1}}{n!}.$$

よって，

$$\frac{d^lP_{1,\chi}}{dt^l}(0) = P_{1,\chi}^{(l)}(0) = -g(\chi)\frac{1}{l+1}B_{l+1,\overline{\chi}} \tag{8.4}$$

である．

さて，$P_{k,\chi}(0)$ の公式を求めよう．ここで

$$Q_{k,a}(t) = \frac{1}{(1-\zeta^a e^t)^k}$$

とおくと，

$$P_{k,\chi}(t) = \sum_{a=1}^{f}\chi(a)Q_{k,a}(t)$$

であり，

$$\frac{d}{dt}Q_{k,a}(t) = k(Q_{k+1,a}(t) - Q_{k,a}(t))$$

であるから，帰納的に $Q_{k,a}(t)$ が $Q_{1,a}(t)$ の高階の微分で表され，よって，$P_{k,\chi}(t)$ も $P_{1,\chi}(t)$ の高階の微分で表されることになる．より具体的には第 1 種スターリング数（定義は 2.1 節参照）を用いて次のように表される．

命題 8.6
$$Q_{k,a}(t) = \frac{1}{(k-1)!}\sum_{l=0}^{k-1}\begin{bmatrix} k \\ l+1 \end{bmatrix} Q_{1,a}^{(l)}(t),$$
$$P_{k,\chi}(t) = \frac{1}{(k-1)!}\sum_{l=0}^{k-1}\begin{bmatrix} k \\ l+1 \end{bmatrix} P_{1,\chi}^{(l)}(t).$$

証明 k についての帰納法による．$k=1$ では正しい．k まで正しいとすれば，$Q_{k+1,a}(t)$ における $Q_{1,a}^{(l)}(t)$ の係数は，$0 \le l \le k$ に対して
$$\frac{1}{(k-1)!}\left\{\begin{bmatrix} k \\ l+1 \end{bmatrix} + \frac{1}{k}\begin{bmatrix} k \\ l \end{bmatrix}\right\}$$
であるが，第 1 種スターリング数の漸化式（25 ページ (2.2) 式）によってこれは
$$\frac{1}{k!}\begin{bmatrix} k+1 \\ l+1 \end{bmatrix}$$
に等しい．よって証明された． ∎

系 8.7
$$P_{k,\chi}(0) = \sum_{a=1}^{f}\frac{\chi(a)}{(1-\zeta^a)^k}$$
$$= -\frac{g(\chi)}{(k-1)!}\sum_{l=0}^{k-1}\begin{bmatrix} k \\ l+1 \end{bmatrix}\frac{B_{l+1,\overline{\chi}}}{l+1}. \tag{8.5}$$

証明 命題の第 2 式で $t=0$ とおいて (8.4) 式を用いればよい． ∎

例 8.8 たとえば，
$$\sum_{a=1}^{f-1}\frac{\chi(a)}{(1-\zeta^a)} = -g(\chi)B_{1,\overline{\chi}},$$
$$\sum_{a=1}^{f-1}\frac{\chi(a)}{(1-\zeta^a)^2} = -g(\chi)(B_{1,\overline{\chi}} + \frac{1}{2}B_{2,\overline{\chi}}),$$
$$\sum_{a=1}^{f-1}\frac{\chi(a)}{(1-\zeta^a)^3} = -g(\chi)(B_{1,\overline{\chi}} + \frac{3}{4}B_{2,\overline{\chi}} + \frac{1}{6}B_{3,\overline{\chi}})$$
である．

以上では，最終的に $P_{1,\chi}^{(l)}(0)$ の評価でベルヌーイ数を扱うために，χ を原始的な指標としたが，その他の点では，この仮定を本質的に使ったわけではない．たとえば以上で任意の a について $\chi(a)$ のかわりに 1 をとってもほとんど同じ計算が実行できて，

$$\sum_{a=1}^{f-1} \frac{1}{1-\zeta^a e^t} = \frac{f}{1-e^{ft}} - \frac{1}{1-e^t}$$
$$= f - \frac{fe^{ft}}{e^{ft}-1} - (1 - \frac{e^t}{e^t-1})$$
$$= f - 1 + \sum_{n=1}^{\infty} B_n \frac{(1-f^n)t^{n-1}}{n!}$$

である．よって $t=0$ とおけば，$B_1 = 1/2$ より，

$$\sum_{a=1}^{f-1} \frac{1}{1-\zeta^a} = \frac{f-1}{2} \tag{8.6}$$

である．$f=p$ が 8.1 節の公式であった．前と類似の計算を実行するには，たとえば

$$\sum_{a=1}^{f-1} Q_{1,a}^{(l)}(0) = \frac{1}{l+1}(1-f^{l+1})B_{l+1} + \delta_{l0}(f-1)$$

（ただし δ_{l0} はクロネッカーのデルタ，すなわち $l=0$ ならば 1，それ以外では 0）に注意して，次の公式が得られる．

補題 8.9

$$\sum_{a=1}^{f-1} \frac{1}{(1-\zeta^a)^k} = \sum_{a=1}^{f-1} Q_{k,a}(0)$$
$$= \frac{1}{(k-1)!} \sum_{l=0}^{k-1} \begin{bmatrix} k \\ l+1 \end{bmatrix} \left\{ \frac{1}{l+1}(1-f^{l+1})B_{l+1} + (f-1)\delta_{l0} \right\}.$$

この公式の例をあげよう．

例 8.10

$$\sum_{a=1}^{f-1} \frac{1}{1-\zeta^a} = \frac{f-1}{2},$$
$$\sum_{a=1}^{f-1} \frac{1}{(1-\zeta^a)^2} = -\frac{(f-1)(f-5)}{12},$$
$$\sum_{a=1}^{f-1} \frac{1}{(1-\zeta^a)^3} = -\frac{(f-1)(f-3)}{8},$$
$$\sum_{a=1}^{f-1} \frac{1}{(1-\zeta^a)^4} = \frac{(f-1)(f^3+f^2-109f+251)}{720}.$$

類似の手法を用いて，

$$\sum_{c=0}^{f-1} c^k \zeta^{ca}$$

という形の和を記述する公式を与えよう．これは a が f で割り切れれば，$\zeta^{ac}=1$ であるから，べき乗の和を表す公式になる．また，a が f で割り切れないという仮定のもとでは，これを $Q_{k,a}(0)$ で表す公式を与える．これは，補題 8.5 の右辺を左辺で表示すると考えた公式の一般化である．(この公式は後で指数和の計算に利用される.) 通常のとおり，自然数 k, j について，$\binom{k}{j}$ は 2 項係数

$$\binom{k}{j} = \frac{k(k-1)\cdots(k-j+1)}{j!}$$

を表すとする．また $j=0$ ならば $\binom{k}{0}=1$ とおく．

補題 8.11

(1) a が f で割り切れるとき，

$$\sum_{c=0}^{f} c^k \zeta^{ac} = \sum_{c=0}^{f} c^k = \sum_{j=0}^{k} \binom{k}{j} B_j \frac{f^{k-j+1}}{k-j+1}$$

である．

(2) a が f で割り切れないとき，

$$\sum_{c=0}^{f} c^k \zeta^{ac} = \sum_{m=1}^{k} (-1)^m (m-1)! Q_{m,a}(0) \left(\sum_{j=1}^{k-m+1} (-1)^{k-j} f^j \binom{k}{j} \left\{ \begin{matrix} k-j+1 \\ m \end{matrix} \right\} \right)$$

となる．

証明 まず a は任意の整数として，わかりやすい関数を微分することにより c^k を抽出するために，t を変数として次のような変形を考える．

$$\begin{aligned}
\sum_{c=0}^{f-1} c^k \zeta^{ca} e^{ct} &= \frac{d^k}{dt^k} \left(\sum_{c=0}^{f-1} \zeta^{ac} e^{ct}\right) \\
&= \frac{d^k}{dt^k} \left(\frac{1-e^{ft}}{1-\zeta^a e^t} \right) \\
&= Q_{1,a}^{(k)}(t) - \sum_{j=0}^{k} \binom{k}{j} f^{k-j} e^{ft} Q_{1,a}^{(j)}(t). \qquad (8.7)
\end{aligned}$$

最後の等式は積の高階微分についてのライプニッツ[3]の公式を用いた．

もし $f|a$ ならば

$$Q_{1,a}(t) = Q_{1,0}(t) = -\frac{1}{e^t-1} = 1 - \frac{e^t}{e^t-1} = 1 - \sum_{n=0}^{\infty} \frac{B_n}{n!} t^{n-1}$$

である（これ自身は $t=0$ で極をもつ）．よってこのとき，(8.7) 式の両辺の t に関するべき級数展開の定数項を比較すると，

$$Q_{1,a}^{(0)}(t) = -\frac{1}{t} + (1-B_1) - \frac{B_2}{2}t - \cdots,$$
$$Q_{1,a}^{(j)}(t) = -\frac{(-1)^j j!}{t^{j+1}} - \frac{B_{j+1}}{j+1} - \frac{B_{j+2}}{(j+2)}t - \cdots \qquad (j \geq 1)$$

に注意して，

$$\begin{aligned}\sum_{c=0}^{f-1} c^k &= -\frac{B_{k+1}}{k+1} + \sum_{j=0}^{k} \binom{k}{j} f^{k-j} \frac{B_{j+1}}{j+1} \\ &\quad + \sum_{j=0}^{k} \binom{k}{j} f^{k-j} \frac{f^{j+1}}{(j+1)!} \cdot (-1)^j j! - f^k \\ &= \sum_{j=0}^{k-1} \binom{k}{j} f^{k-j} \frac{B_{j+1}}{j+1} + \frac{f^{k+1}}{k+1} - f^k \\ &= \sum_{j=0}^{k-1} \binom{k}{j+1} f^{k-j} \frac{B_{j+1}}{k-j} + \frac{f^{k+1}}{k+1} - f^k \\ &= \sum_{j=1}^{k} \binom{k}{j} f^{k-j+1} \frac{B_j}{k-j+1} + \frac{f^{k+1}}{k+1} - f^k.\end{aligned}$$

（第 2 の等号では $\sum_{j=0}^{k}(-1)^j\binom{k}{j}\frac{1}{j+1} = \frac{1}{k+1}$ を用いた．）　よって，

$$\sum_{c=0}^{f} c^k = \sum_{j=0}^{k} \binom{k}{j} B_j \frac{f^{k-j+1}}{k-j+1}.$$

こうして再度べき乗和の公式が得られた．

次に a は f で割り切れないと仮定する．ここで，$Q_{1,a}^{(n)}(t)$ を $Q_{k,a}(t)$ で表したい．これは命題 8.6 で与えた公式の逆であるが，今度は第 2 種スターリング数（定義は 2.1 節）を用いて表される．

---

[3] Gottfried Wilhelm Freiherr von Leibniz（1646.7.1 ドイツ Leipzig 生——1716.11.14 ドイツ Hannover 没）

28 ページ命題 2.6 の公式 (5.1) において $m \to m+1$, $n \to k+1$ とすると,

$$\delta_{m+1,k+1}\ (=\delta_{m,k}) = (-1)^{k+1}\sum_{l=m+1}^{k+1}(-1)^l \begin{Bmatrix} k+1 \\ l \end{Bmatrix} \begin{bmatrix} l \\ m+1 \end{bmatrix}.$$

これと命題 8.6 より,

$$\begin{aligned} Q_{1,a}^{(k)}(t) &= \sum_{m=0}^{k} \delta_{m,k} Q_{1,a}^{(m)}(t) \\ &= \sum_{m=0}^{k}(-1)^{k+1}\sum_{l=m+1}^{k+1}(-1)^l \begin{Bmatrix} k+1 \\ l \end{Bmatrix} \begin{bmatrix} l \\ m+1 \end{bmatrix} Q_{1,a}^{(m)}(t) \\ &= \sum_{l=1}^{k+1}(-1)^{k+l+1}\begin{Bmatrix} k+1 \\ l \end{Bmatrix} \sum_{m=0}^{l-1} \begin{bmatrix} l \\ m+1 \end{bmatrix} Q_{1,a}^{(m)}(t) \\ &= \sum_{l=1}^{k+1}(-1)^{k+l+1}(l-1)!\begin{Bmatrix} k+1 \\ l \end{Bmatrix} Q_{l,a}(t). \end{aligned}$$

よって, (8.7) 式で $t=0$ とおいて

$$\begin{aligned} \sum_{c=0}^{f-1} c^k \zeta^{ac} &= \sum_{m=1}^{k+1}(-1)^{k+m+1}(m-1)!\begin{Bmatrix} k+1 \\ m \end{Bmatrix} Q_{m,a}(0) \\ &\quad + \sum_{j=0}^{k}\binom{k}{j} f^j \sum_{m=1}^{k-j+1}(-1)^{k-j+m}(m-1)!\begin{Bmatrix} k-j+1 \\ m \end{Bmatrix} Q_{m,a}(0) \\ &= \sum_{j=1}^{k}\binom{k}{j} f^j \sum_{m=1}^{k-j+1}(-1)^{k-j+m}(m-1)!\begin{Bmatrix} k-j+1 \\ m \end{Bmatrix} Q_{m,a}(0) \\ &= \sum_{m=1}^{k}(-1)^m (m-1)! Q_{m,a}(0)\left(\sum_{j=1}^{k-m+1}(-1)^{k-j} f^j \binom{k}{j}\begin{Bmatrix} k-j+1 \\ m \end{Bmatrix}\right). \end{aligned}$$

∎

以上の計算により, たとえば次がわかる.

例 8.12

$$\sum_{c=0}^{f-1} c\zeta^{ac} = -\frac{f}{1-\zeta^a},$$

$$\sum_{c=0}^{f-1} c^2\zeta^{ac} = \frac{-f^2+2f}{1-\zeta^a} - \frac{2f}{(1-\zeta^a)^2},$$

$$\sum_{c=0}^{f-1} c^3\zeta^{ac} = \frac{-f^3+3f^2-3f}{1-\zeta^a} + \frac{-3f^2+9f}{(1-\zeta^a)^2} + \frac{-6f}{(1-\zeta^a)^3}.$$

このような公式の応用は次の節で述べる．

8.4 和のさまざまな例

この節ではいくつか散発的な例を述べてみる．1のべき根ではなく，指標に関する和で与えられたものについても類似の手法が使えることがある．これを見てみたい．χ を f を法とする原始的なディリクレ指標とする．次の和を考える．

$$S_k(\chi) = \sum_{a_1,\cdots,a_k=0}^{f-1} \chi(a_1+\cdots+a_k)a_1\cdots a_k.$$

ここで注意すべきは，和は a_i の動く自然数の範囲に依存している点（すなわち，$\bmod f$ の代表を取り替えると値がかわってしまう点）である．この和をいきなり場合分けなどして求めるのは，たとえば $k=2$ のときに限ってみても，かなり効率が悪い．まず次に着目しよう（(8.2) 式）．

$$\chi(a) = g(\overline{\chi})^{-1} \sum_{n=1}^{f} \overline{\chi(n)}\zeta^{an}.$$

これを用いれば，

$$S_k(\chi) = g(\overline{\chi})^{-1} \sum_{a_1,\cdots,a_k=0}^{f-1} \sum_{n=1}^{f} \overline{\chi(n)}\zeta^{n(a_1+\cdots+a_k)}a_1\cdots a_k \tag{8.8}$$

であるが，

$$\sum_{a=0}^{f-1} a\zeta^{an} = -\frac{f}{1-\zeta^n}$$

であったから，

$$\begin{aligned} S_k(\chi) &= (-f)^k g(\overline{\chi})^{-1} \sum_{n=1}^{f} \frac{\overline{\chi(n)}}{(1-\zeta^n)^k} \\ &= (-f)^k g(\overline{\chi})^{-1} P_{k,\overline{\chi}}(0) \\ &= \frac{(-1)^{k+1}f^k}{(k-1)!} \sum_{l=0}^{k-1} \frac{1}{l+1} \begin{bmatrix} k \\ l+1 \end{bmatrix} B_{l+1,\chi}. \end{aligned}$$

たとえば，

$$S_2(\chi) = -f^2(B_{1,\chi} + \frac{1}{2}B_{2,\chi}),$$

$$S_3(\chi) = f^3(B_{1,\chi} + \frac{3}{4}B_{2,\chi} + \frac{1}{6}B_{3,\chi})$$

である.

類似の例として，次のような和を考えよう.

$$S(\chi, e_1, \cdots, e_k) = \sum_{a_1,\cdots,a_k=1}^{f-1} \chi(a_1+\cdots+a_k)a_1^{e_1}\cdots a_k^{e_k}.$$

これをベルヌーイ数の和で表す公式も前とほぼ同様の方法で求められる．実際，前と同様，指標をガウス和と 1 のべき根で表して，

$$S(\chi, e_1, \cdots, e_k) = g(\overline{\chi})^{-1}\sum_{n=1}^{f}\overline{\chi(n)}\prod_{j=1}^{k}(\sum_{c=1}^{f-1}c^{e_j}\zeta^{cn})$$

$$= g(\overline{\chi})^{-1}\sum_{n=1}^{f}\overline{\chi(n)}\sum_{\substack{1\le l_j\le e_j\\ 1\le m_j\le e_j-l_j+1\\ 1\le j\le k}}(-1)^{e_1+\cdots+e_k-l_1-\cdots-l_k}f^{l_1+\cdots+l_k}\binom{e_1}{l_1}\cdots\binom{e_k}{l_k}$$

$$\times(-1)^{m_1+\cdots+m_k}Q_{m_1+\cdots+m_k,n}(0)(m_1-1)!\cdots(m_k-1)!$$

$$\times\left\{{e_1-l_1+1 \atop m_1}\right\}\cdots\left\{{e_k-l_k+1 \atop m_k}\right\}$$

$$= -\sum_{\substack{1\le l_j\le e_j\\ 1\le m_j\le e_j-l_j+1\\ 1\le j\le k}}(-1)^{e_1+\cdots+e_k-l_1-\cdots-l_k}f^{l_1+\cdots+l_k}\binom{e_1}{l_1}\cdots\binom{e_k}{l_k}$$

$$\times\frac{(-1)^{m_1+\cdots+m_k}}{(m_1+\cdots+m_k-1)!}(m_1-1)!\cdots(m_k-1)!$$

$$\times\left\{{e_1-l_1+1 \atop m_1}\right\}\cdots\left\{{e_k-l_k+1 \atop m_k}\right\}$$

$$\times\left(\sum_{l=0}^{m_1+\cdots+m_k-1}\frac{1}{l+1}\left[{m_1+\cdots+m_k \atop l+1}\right]B_{l+1,\chi}\right).$$

以上を再度，公式としてまとめておく.

補題 8.13　次の公式が成り立つ.

$$S(\chi, e_1, \cdots, e_k) = (-1)^{e_1+\cdots+e_k+1} \sum_{l_1=1}^{e_1} \cdots \sum_{l_k=1}^{e_k} (-f)^{l_1+\cdots+l_k} \prod_{j=1}^{k} \binom{e_j}{l_j}$$
$$\times \sum_{m_1=1}^{e_1-l_1+1} \cdots \sum_{m_k=1}^{e_k-l_k+1} \frac{(-1)^{m_1+\cdots+m_k}}{(m_1+\cdots+m_k-1)!} \prod_{j=1}^{k} (m_j-1)! \left\{ \begin{matrix} e_j - l_j + 1 \\ m_j \end{matrix} \right\}$$
$$\times \left(\sum_{l=0}^{m_1+\cdots+m_k-1} \frac{1}{l+1} \begin{bmatrix} m_1+\cdots+m_k \\ l+1 \end{bmatrix} B_{l+1,\chi} \right),$$
$$S(\chi) = S(\chi, 1, \cdots, 1) = \frac{(-1)^{k+1} f^k}{(k-1)!} \sum_{l=0}^{k-1} \frac{1}{l+1} \begin{bmatrix} k \\ l+1 \end{bmatrix} B_{l+1,\chi}.$$

たとえば

$$S(\chi, 2, 1) = \sum_{m,n=0}^{f-1} \chi(m+n) m^2 n = -f^2 (f B_{1,\chi} + \frac{(f+1)}{2} B_{2,\chi} + \frac{1}{3} B_{3,\chi})$$

となる.

さらに類似の例として，m を固定された f と素な f より小さい自然数として，

$$D_m(\chi) = \sum_{a=1}^{f} \chi(a+m) a$$

を考える.

$$D_m(\chi) = g(\bar{\chi})^{-1} \sum_{a,n=1}^{f} a \bar{\chi}(n) \zeta^{(a+m)n}$$
$$= g(\bar{\chi})^{-1} \left(\sum_{n=1,(n,f)=1}^{f} \bar{\chi}(n) \zeta^{mn} \left(-\frac{f}{(1-\zeta^n)} + f \right) \right)$$

であるが

$$\sum_{n=1,(n,f)=1}^{f} \bar{\chi}(n)(1-\zeta^{mn})(1-\zeta^n)^{-1} = \sum_{l=0}^{m-1} \sum_{n=1,(n,f)=1}^{f} \bar{\chi}(n) \zeta^{nl} = g(\bar{\chi}) \sum_{l=1}^{m-1} \chi(l)$$

であるから，前節の $\sum_{n=1}^{f} \bar{\chi}(n)(1-\zeta^n)^{-1} = -g(\bar{\chi}) B_{1,\chi}$ と合わせて

$$D_m(\chi) = f(\sum_{l=1}^{m} \chi(l) + B_{1,\chi})$$

となる.

このほかいくつか類例をあげておく．証明は読者の演習にまかせ，ここでは省略する．

例 8.14

(1)　次が成り立つ．

$$\sum_{a=1}^{f-1} \frac{\chi(a)\zeta^a}{(1-\zeta^a)^2} = -\frac{1}{2} g(\chi) B_{2,\overline{\chi}},$$

$$\sum_{a=1}^{f-1} \frac{\chi(a)\zeta^a(1+\zeta^a)}{(1-\zeta^a)^3} = -\frac{1}{3} g(\chi) B_{3,\overline{\chi}}.$$

(2)　$\psi(n) = (\frac{n}{p})$ を平方剰余指標とするとき，次が成り立つ．

$$\sum_{m,n=0}^{p-1} \psi(m+n)\psi(m)mn = \frac{1}{2}(p^2 B_{1,\psi}^2 - \frac{p(p-1)(7p+1)}{12}).$$

(3)　次が成り立つ．

$$\sum_{l,m,n=0}^{p-1} \psi(lm+mn+nl) = \psi(-1)p(p-1),$$

$$\sum_{l,m,n=0}^{p-1} \psi(lm+mn+nl)l = \psi(-1)\frac{p^2(p-1)}{2},$$

$$\sum_{l,m,n=0}^{p-1} \psi(lm+mn+nl)l^2 = \psi(-1)\frac{p^2(p-1)(2p-1)}{6},$$

$$\sum_{l,m,n=0}^{p-1} \psi(lm+mn+nl)l^3 = \psi(-1)\frac{p^3(p-1)^2}{4},$$

$$\sum_{l,m,n=0}^{p-1} \psi(lm+mn+nl)lm = \psi(-1)\frac{p^2(p^2-1)}{6},$$

$$\sum_{l,m,n=0}^{p-1} \psi(lm+mn+nl)l^2 m = \psi(-1)\frac{p^3(p^2-1)}{12},$$

$$\sum_{l,m,n=0}^{p-1} \psi(lm+mn+nl)lmn = -\frac{3p^3}{2}(B_{1,\psi})^2 + \psi(-1)\frac{p^3(p-1)}{4}.$$

（ヒント：$\sum_{n=0}^{p-1} \psi(n(l+m)+lm)$ は $l+m \not\equiv \bmod p$ ならば 0 である．最後の式では，l, m, n を $p-l, p-m, p-n$ に置き換えてもとの式に加えよ．）

8.5　散発的な例 1：関数を使う

補題 8.15　$f>1$，かつ f は奇数とし，χ を f を導手とする原始的指標とすると，

$$\sum_{a=1}^{f-1}\frac{\chi(a)}{(1-\zeta^a)(1-\zeta^{2a})^2} = -g(\chi)\left(\frac{1}{24}B_{3,\bar{\chi}}+\frac{1}{4}(1+\overline{\chi(2)})B_{2,\bar{\chi}}+\frac{1}{8}(3+5\overline{\chi(2)})B_{1,\bar{\chi}}\right)$$

となる．

証明

$$Q_{k,\chi}(t)=\sum_{a=1}^{f}\frac{\chi(a)(1+\zeta^a e^t)}{(1-\zeta^{2a}e^{2t})^k},$$

$$P_{k,\chi}(t)=\sum_{a=1}^{f}\frac{\chi(a)}{(1-\zeta^a e^t)^k}$$

とおくと，

$$Q_{1,\chi}(t)=P_{1,\chi}(t)=-g(\chi)\sum_{n=1}^{\infty}B_{n,\bar{\chi}}\frac{t^{n-1}}{n!}.$$

$$\frac{d}{dt}Q_{k,\chi}(t)=2kQ_{k+1,\chi}(t)+(1-2k)Q_{k,\chi}(t)-\overline{\chi(2)}P_{k,\chi}(2t).$$

よって，帰納的に $Q_{k,\chi}(0)$ は $P_{k,\chi}(0)$ で表示され，よってベルヌーイ数で表示される．たとえば，上の関係式で $k=1$ として，その微分をとることにより

$$Q'_{1,\chi}(t)=2Q_{2,\chi}(t)-Q_{1,\chi}(t)-\overline{\chi(2)}P_{1,\chi}(2t),$$
$$Q'_{2,\chi}(t)=\frac{1}{2}(Q''_{1,\chi}(t)+Q'_{1,\chi}(t))+\overline{\chi(2)}P'_{1,\chi}(2t)$$

によって

$$Q_{2,\chi}(0)=-\frac{g(\chi)}{2}(\frac{1}{2}B_{2,\overline{\chi}}+(1+\overline{\chi(2)})B_{1,\overline{\chi}}),$$
$$Q'_{2,\chi}(0)=-\frac{g(\chi)}{2}(\frac{1}{3}B_{3,\overline{\chi}}+(\frac{1}{2}+\overline{\chi(2)})B_{2,\overline{\chi}})$$

となる．同様にして，

$$Q'_{2,\chi}(t)=4Q_{3,\chi}(t)-3Q_{2,\chi}(t)-\overline{\chi(2)}P_{2,\chi}(2t)$$

より

$$Q_{3,\chi}(0)=\frac{1}{4}(Q'_{2,\chi}(0)+3Q_{2,\chi}(0)+\overline{\chi(2)}P_{2,\chi}(0)).$$

補題の左辺は $Q_{3,\chi}(0)$ に等しいから，これに上記の値と $P_{2,\chi}(0)=-g(\chi)(B_{1,\overline{\chi}}+B_{2,\overline{\chi}}/2)$ を代入すれば右辺の値となる． ∎

8.6 散発的な例 2：対称性の利用

以下の例において，$\psi(n)=(\frac{n}{p})$ は平方剰余指標とする．

例 8.16

$$I=\sum_{a=1}^{p-1}\psi(a)a$$

とおく．定義により，これは $pB_{1,\psi}$ に等しい．

もし $p\equiv 1 \bmod 4$ ならば $I=0$ となる．これは次のように簡単に計算される．a を $p-a$ で置き換えて，$\psi(a)=\psi(-a)=\psi(p-a)$ より，

$$\begin{aligned}I&=\sum_{a=1}^{p-1}\psi(p-a)(p-a)\\&=\sum_{a=1}^{p-1}\psi(a)(p-a).\end{aligned}$$

よって，もとの表示と加えて，

$$\begin{aligned}2I&=\sum_{a=1}^{p-1}\psi(a)(a+p-a)\\&=p\sum_{a=1}^{p-1}\psi(a)=0.\end{aligned}$$

このような論法は $p\equiv 3 \bmod 4$ ならばもちろん使えない．実際，$p\equiv 3 \bmod 4$ で $p>3$ ならば $-I/p$ が虚 2 次体 $\mathbf{Q}(\sqrt{-p})$ の類数になるので，もっと複雑な量である．

さて，上のような置き換えが計算上有効なことは非常に多い．たとえば

例 8.17　ψ を上のとおりとし，

$$I=\sum_{l,m,n=1,4ln\equiv m^2 \bmod p}^{p-1}\psi(l)lmn$$

とおくと，$m\to p-m$ として，

$$
\begin{aligned}
2I &= \sum_{l,m,n=1,4ln\equiv m^2 \bmod p}^{p-1} \psi(l)ln(m+p-m) \\
&= p\sum_{l,n=1}^{p-1} \psi(l)l(\psi(ln)+1)n \\
&= p\sum_{l,n=1}^{p-1} (l\psi(n)n+\psi(l)ln) \\
&= p^3(p-1)B_{1,\psi}.
\end{aligned}
$$

よって，

$$
I = \frac{p^3(p-1)}{2}B_{1,\psi}
$$

となる．

例 8.18　次の和は保型形式の次元公式との関連で考えられたものである ([83])．$\psi(n) = \left(\frac{n}{p}\right)$ として，

$$
S = \{(s,t,r) \in \mathbf{F}_p^3;\ s(r+s)(s+t) \neq 0\}
$$

とおく．$\zeta = e^{2\pi i/p}$ とし，

$$
I = \sum_{(s,t,r)\in S} \frac{\psi(s^2-rt)}{(\zeta^{r+s}-1)(\zeta^{s+t}-1)(\zeta^{-s}-1)}
$$

と和を定義する．この和の初等的な計算法は知られていなかったようであるが，次のように，単純に計算できる．$a=r+s$, $b=s+t$, $c=-s$ と置き換えて，$s^2-rt=c^2-(a+c)(b+c)=-ab-bc-ca$．よって，$T=\mathbf{F}_p^{\times 3}$ とおいて，さらに a, b, c を $-a$, $-b$, $-c$ に置き換える計算を実行すれば，

$$
\begin{aligned}
I &= \sum_{(a,b,c)\in T} \frac{\psi(-ab-bc-ca)}{(\zeta^a-1)(\zeta^b-1)(\zeta^c-1)} \\
&= \sum_{(a,b,c)\in T} \frac{\psi(-ab-bc-ca)}{(\zeta^{-a}-1)(\zeta^{-b}-1)(\zeta^{-c}-1)} \\
&= \sum_{(a,b,c)\in T} \frac{\psi(-ab-bc-ca)\zeta^a\zeta^b\zeta^c}{(1-\zeta^a)(1-\zeta^b)(1-\zeta^c)} \\
&= -\sum_{(a,b,c)\in T} \frac{\psi(-ab-bc-ca)(\zeta^a-1+1)(\zeta^b-1+1)(\zeta^c-1+1)}{(\zeta^a-1)(\zeta^b-1)(\zeta^c-1)}.
\end{aligned}
$$

よって，分子を展開して同じ項を左辺に移項すれば，

$$2I = -\sum_{(a,b,c)\in T} \psi(-ab-bc-ca) \times \left(\frac{1}{(1-\zeta^a)(1-\zeta^b)} + \frac{1}{(1-\zeta^b)(1-\zeta^c)} + \frac{1}{(1-\zeta^c)(1-\zeta^a)} - \frac{1}{1-\zeta^a} - \frac{1}{1-\zeta^b} - \frac{1}{1-\zeta^c} + 1\right)$$

となる．a, b を固定すれば，

$$\sum_{c\in\mathbf{F}_p^\times} \psi(-ab-(a+b)c) = \begin{cases} -\psi(-ab) & a+b\neq 0 \text{ のとき}, \\ (p-1)\psi(-ab) = (p-1) & a=-b\neq 0 \text{ のとき}. \end{cases}$$

ゆえに，$a\neq 0$ を固定すれば

$$\sum_{b,c=1}^{p-1} \psi(-ab-bc-ca) = (p-1) - \sum_{b\neq -a,\ b\neq 0} \psi(-ab) = p.$$

ここで例 8.8，例 8.10 により

$$\sum_{a,b\in\mathbf{F}_p^\times} \frac{\psi(-ab)}{(1-\zeta^a)(1-\zeta^b)} = \psi(-1)g(\psi)^2 B_{1,\psi}^2 = pB_{1,\psi}^2,$$

$$p\sum_{a\in\mathbf{F}_p^\times} \frac{1}{(1-\zeta^a)(1-\zeta^{-a})} = \frac{p(p-1)}{2} + \frac{p(p-1)(p-5)}{12}.$$

ゆえに $p-1 = p-\psi(a^2)$ に注意して

$$\sum_{(a,b,c)\in T} \psi(-ab-bc-ca)\frac{1}{(1-\zeta^a)(1-\zeta^b)} = -pB_{1,\psi}^2 + \frac{p(p-1)(p-5)}{12} + \frac{p(p-1)}{2}$$

である．また，

$$\sum_{(a,b,c)\in T} \frac{\psi(-ab-bc-ca)}{1-\zeta^a} = \frac{p(p-1)}{2},$$

$$\sum_{(a,b,c)\in T} \psi(-ab-bc-ca) = p(p-1).$$

よって，全体をまとめると，

$$
\begin{aligned}
I &= \frac{3}{2}pB_{1,\psi}^2 - \frac{p(p-1)(p-5)}{8} - \frac{p(p-1)}{2} \\
&= \frac{3}{2}pB_{1,\psi}^2 - \frac{p(p-1)^2}{8}.
\end{aligned}
$$

特に，$p \equiv 1 \bmod 4$ ならば $B_{1,\psi} = 0$ であり，また $p \equiv 3 \bmod 4$ で $p > 3$ ならば $B_{1,\psi} = -h(-p)$（$h(-p)$ は虚 2 次体 $\mathbf{Q}(\sqrt{-p})$ の類数）であるから，I の類数による表示が存在する．

例 8.19　$S = \{(a,b,c) \in \mathbf{Z}^3; 1 \leq a,b,c \leq p-1, ab+bc+ca \equiv 0 \bmod p\}$ とおき

$$
I = \sum_{(a,b,c)\in S} \psi(abc)abc
$$

とする．I は和の条件が複雑で計算は単純でない．しかしさらに $\psi(-1) = 1$ と仮定すると，I は次のようにして計算できる．

$$
I = \sum_{(a,b,c)\in S} \psi(-abc)(p-a)(p-b)(p-c)
$$

より

$$
\begin{aligned}
2I &= \sum_{(a,b,c)\in S} \psi(abc)((p-a)(p-b)(p-c) + abc) \\
&= \sum_{(a,b,c)\in S} \psi(abc)(p^3 - p^2(a+b+c) + p(ab+bc+ca)).
\end{aligned}
$$

しかし $\psi(abc) = \psi(-c^2(a+b)) = \psi(a+b)$ であるから S の条件が a, b, c について対称なことより

$$
\begin{aligned}
\sum_{(a,b,c)\in S} \psi(abc)(ab+bc+ca) &= 3\sum_{(a,b,c)\in S} \psi(a+b)ab \\
&= 3\sum_{a,b,a+b\not\equiv 0 \bmod p} \psi(a+b)ab \\
&= 3\sum_{a,b=1}^{p-1} \psi(a+b)ab = -3p^2\left(B_{1,\psi} + \frac{1}{2}B_{2,\psi}\right).
\end{aligned}
$$

実は，いまは $\psi(-1) = 1$ より $B_{1,\psi} = 0$ である．また，

$$\sum_{(a,b,c)\in S}\psi(a+b)(a+b+c)=3\sum_{a=1}^{p-1}(\sum_{b=1}^{p-1}\psi(a+b))a$$
$$=-3\sum_{a=1}^{p-1}\psi(a)a=-3pB_{1,\psi}$$

であり，これは 0 である．

$$\sum_{a,b,c\in S}\psi(a+b)=\sum_{a,b=1}^{p-1}\psi(a+b)=\sum_{a=1}^{p-1}(-\psi(a))=0.$$

よって，

$$I=-\frac{3p^3}{4}B_{2,\psi}$$

である．

注意 8.20 $\psi(-1)=-1$ ならば，このように I を一般ベルヌーイ数で表す簡単な公式は予想としてしか知られていない．

8.7 散発的な例 3：非対称なものを対称にする

$\psi(x)$ を法 p の平方剰余指標として，次のような特殊な和を考える．

$$I=\sum_{m,n=1}^{p-1}\psi(m-4n)\psi(m)mn.$$

この和の公式は [82]，[30] で，跡公式と代数幾何の比較により与えられたものであるが，初等的に計算することもできる．以下これを計算してみよう．上で $m-4n$ の部分が n ならば和は単純で

$$\sum_{m,n=1}^{p-1}\psi(mn)mn=\left(\sum_{m=1}^{p-1}\psi(m)m\right)^2=p^2B_{1,\psi}^2$$

となる．しかし，上の和は微妙に対称性が崩れていてこのままでは計算ができない．これを指数和に書き換え，そこで対称的な形に変形することにより計算を実行する．

$$\psi(m) = g(\psi)^{-1}\sum_{a=1}^{p-1}\psi(a)\zeta^{am}, \quad \psi(m-4n) = g(\psi)^{-1}\sum_{b=1}^{p-1}\psi(b)\zeta^{b(m-4n)}$$

より，

$$I = g(\psi)^{-2}\sum_{a,b=1}^{p-1}\psi(ab)\sum_{m,n=1}^{p-1}mn\zeta^{am+b(m-4n)}.$$

しかし，$c \notin p\mathbf{Z}$ については $\sum_{m=1}^{p-1} m\zeta^{cm} = -\frac{p}{1-\zeta^c}$ であったから，

$$\begin{aligned}
I &= g(\psi)^{-2}\left(p^2 \sum_{a,b=1,\ a\not\equiv -b \bmod p}^{p-1}\frac{\psi(ab)}{(1-\zeta^{-4b})(1-\zeta^{a+b})}\right.\\
&\qquad \left. + \psi(-1)\sum_{m,n,b=1}^{p-1} mn\zeta^{-4nb}\right)\\
&= p\psi(-1)\sum_{a,b=1,\ a+b\neq p}^{p-1}\frac{\psi(ab)}{(1-\zeta^{-4b})(1-\zeta^{a+b})} - \frac{p(p-1)^2}{4}\\
&\qquad\qquad (g(\psi)^2 = \psi(-1)p).
\end{aligned}$$

以上により I を求めるには

$$J = \psi(-1)\sum_{a,b=1,\ a+b\neq p}^{p-1}\frac{\psi(ab)}{(1-\zeta^{-4b})(1-\zeta^{a+b})}$$

を求めればよい．さて，この和 J が求めにくい理由の 1 つは，和が a, b について対称でないことである．そこで対称なように書き換えることを考える．a, b を入れ替えても単に記号を変更するだけだから

$$J = \psi(-1)\sum_{a,b=1,\ a+b\neq p}^{p-1}\frac{\psi(ab)}{(1-\zeta^{-4a})(1-\zeta^{b+a})}$$

となる．ここで両方の表示を加えて平均をとりたい．これを計算するために次の等式に注意しよう．

$$\begin{aligned}
\frac{1}{1-\zeta^{-4a}} + \frac{1}{1-\zeta^{-4b}} &= \frac{2-\zeta^{-4a}-\zeta^{-4b}}{(1-\zeta^{-4a})(1-\zeta^{-4b})} = \frac{2\zeta^{4a+4b}-\zeta^{4a}-\zeta^{4b}}{(1-\zeta^{4a})(1-\zeta^{4b})}\\
&= \frac{\zeta^{4a+4b}-1+(1-\zeta^{4a})(1-\zeta^{4b})}{(1-\zeta^{4a})(1-\zeta^{4b})}\\
&= 1 - \frac{1-\zeta^{4a+4b}}{(1-\zeta^{4a})(1-\zeta^{4b})}.
\end{aligned}$$

つまりは

$$J_1 = \sum_{a,b=1,a+b\neq p}^{p-1} \frac{\psi(ab)}{1-\zeta^{a+b}},$$

$$J_2 = \sum_{a,b=1,a+b\neq p}^{p-1} \frac{\psi(ab)(1-\zeta^{4a+4b})}{(1-\zeta^{4a})(1-\zeta^{4b})(1-\zeta^{a+b})}$$

とおくと

$$J = \frac{\psi(-1)}{2}(J_1 - J_2)$$

である．ここで

$$\begin{aligned} J_1 &= -\frac{1}{p}\sum_{k=1}^{p-1}\sum_{a,b=1,a+b\neq p}^{p-1} \psi(ab)k\zeta^{k(a+b)} \\ &= -\frac{1}{p}(g(\psi)^2 - \psi(-1)(p-1)) \times \frac{p(p-1)}{2} = -\frac{\psi(-1)(p-1)}{2}. \end{aligned}$$

また

$$\begin{aligned} J_2 &= \sum_{a,b=1,\ a+b\neq p}^{p-1} \psi(ab)\frac{1-\zeta^{4a+4b}}{(1-\zeta^{4a})(1-\zeta^{4b})(1-\zeta^{a+b})} \\ &= \sum_{a,b=1}^{p-1} \frac{\sum_{l=0}^{3}\psi(ab)\zeta^{l(a+b)}}{(1-\zeta^{4a})(1-\zeta^{4b})} - \sum_{a=1}^{p-1}\frac{4\psi(-1)}{(1-\zeta^{4a})(1-\zeta^{-4a})}. \end{aligned}$$

ここで例 8.10 より

$$\begin{aligned} \sum_{a=1}^{p-1}\frac{1}{(1-\zeta^{4a})(1-\zeta^{-4a})} &= \sum_{a=1}^{p-1}\left(\frac{1}{1-\zeta^{4a}} - \frac{1}{(1-\zeta^{4a})^2}\right) \\ &= \frac{p-1}{2} + \frac{(p-1)(p-5)}{12} = \frac{p^2-1}{12} \end{aligned}$$

となる．さて，

$$\sum_{a=1}^{p-1}\frac{\psi(a)\zeta^{la}}{1-\zeta^{4a}} = -\frac{1}{p}\sum_{a,c=1}^{p-1}\psi(a)c\zeta^{4ac+al} = -\frac{1}{p}g(\psi)\sum_{c=1}^{p-1}\psi(4c+l)c$$

である．ゆえに，$S(l) = \sum_{c=1}^{p-1}\psi(4c+l)c$ とおくと

$$J_2 = \frac{\psi(-1)}{p}\sum_{l=0}^{3}S(l)^2 - \frac{\psi(-1)(p^2-1)}{3}$$

となる．まとめて

$$J = -\frac{p-1}{4} + \frac{p^2-1}{6} - \frac{1}{2p}\sum_{l=0}^{3} S(l)^2 = \frac{(p-1)(2p-1)}{12} - \frac{1}{2p}\sum_{l=0}^{3} S(l)^2$$

となる．次に

$$\sum_{l=0}^{3} S(l)^2 = (\sum_{c=1}^{p-1}\psi(4c)c)^2 + (\sum_{c=1}^{p-1}\psi(4c+1)c)^2 + (\sum_{c=1}^{p-1}\psi(4c+2)c)^2 + (\sum_{c=1}^{p-1}\psi(4c+3)c)^2$$

を計算する必要がある．この計算法はいろいろあるが，ここではなるべく直接計算してみよう．（一般的な計算法については [38] を参照.）　まず，

$$\begin{aligned}
&\sum_{c=1}^{p-1}(\psi(2c)c + \psi(2c+1)c) \\
&= \frac{1}{2}\left(\sum_{c=0}^{p-1}(\psi(2c)\times(2c) + \psi(2c+1)(2c+1)) - \sum_{c=0}^{p-1}\psi(2c+1)\right) \\
&= \frac{1}{2}\left(\sum_{c=1}^{2p-1}\psi(c)c\right) \\
&= \frac{1}{2}\sum_{c=1}^{p-1}\psi(c)(c+c+p) = \sum_{c=1}^{p-1}\psi(c)c
\end{aligned}$$

である．よって，

$$\sum_{c=1}^{p-1}\psi(2c+1)c = (1-\psi(2))\sum_{c=1}^{p-1}\psi(c)c$$

となる．同様に

$$\begin{aligned}
&\sum_{c=1}^{p-1}(\psi(4c)c + \psi(4c+1)c + \psi(4c+2)c + \psi(4c+3)c) \\
&= \frac{1}{4}\sum_{c=1}^{4p-1}\psi(c)c = \sum_{c=1}^{p-1}\psi(c)c
\end{aligned}$$

である．すなわち，

$$\sum_{c=1}^{p-1}(\psi(4c+1) + \psi(4c+3))c = (1-\psi(2))\sum_{c=1}^{p-1}\psi(c)c.$$

ここで，$p \equiv 1 \bmod 4$ の場合と $p \equiv 3 \bmod 4$ の場合を分ける．

最初に $p \equiv 3 \bmod 4$ と仮定すると，$\psi(-1) = -1$ である．よって，$\psi(4c+3) = -\psi(4(p-c)-3) = -\psi(4(p-1-c)+1)$ であり，

$$\sum_{c=0}^{p-1} \psi(4c+3)c = -\sum_{c=0}^{p-1} \psi(4c+1)(p-1-c) = \sum_{c=0}^{p-1} \psi(4c+1)c$$

となる．ゆえにこの場合は

$$\sum_{c=1}^{p-1} \psi(4c+1)c = \sum_{c=1}^{p-1} \psi(4c+3)c = \frac{1-\psi(2)}{2} \sum_{c=1}^{p-1} \psi(c)c.$$

よって，

$$\begin{aligned}\sum_{l=0}^{3} S(l)^2 &= \left(1 + (1-\psi(2))^2 + \frac{(1-\psi(2))^2}{2}\right) \left(\sum_{c=1}^{p-1} \psi(c)c\right)^2 \\ &= (4-3\psi(2))p^2 B_{1,\psi}^2\end{aligned}$$

となる．$p \equiv 3 \bmod 4$ という仮定より，$p \neq 3$ ならば $B_{1,\psi} = -h(-p)$（$h(-p)$ は虚 2 次体 $\mathbf{Q}(\sqrt{-p})$ の類数）である（93 ページ (6.4) 式）．

次に $p \equiv 1 \bmod 4$ とする．このときは，$B_{1,\psi} = 0$ であるから，上の式からは $\sum_{c=1}^{p-1} \psi(4c+1)c$ と $\sum_{c=1}^{p-1} \psi(4c+3)c$ が分離できない．この両者を分離するために 4 を導手とするディリクレ指標 δ を導入する．ここで $x \equiv 3 \bmod 4$ に対して $\delta(x) = -1$ である．ここで $\psi\delta$ は導手が $4p$ の原始的ディリクレ指標となり，定義により

$$\begin{aligned}4pB_{1,\psi\delta} = \sum_{c=0}^{4p-1} \psi(c)\delta(c)c &= \sum_{c=0}^{p-1}(\psi(4c+1)(4c+1) - \psi(4c+3)(4c+3)) \\ &= 4(S(1) - S(3)) = 8S(1) = -8S(3)\end{aligned}$$

である．また，$B_{1,\psi} = 0$ より，$S(0) = S(2) = 0$ である．よって，

$$S(1)^2 + S(3)^2 = \frac{p^2}{2}(B_{1,\psi\delta})^2$$

となる．また，$h(-4p) = -B_{1,\psi\delta}$ である．以上によって

$$I = -\frac{p(p-1)(p-2)}{12} - \begin{cases} 7/2 & p = 3 \text{ のとき}, \\ p^2 \cdot h(-4p)^2/4 & p \equiv 1 \bmod 4 \text{ のとき}, \\ (4-3\psi(2))p^2 \cdot h(-p)^2/2 & p \equiv 3 \bmod 4 \text{ かつ } p \neq 3 \text{ のとき}. \end{cases}$$

なお，この節の内容をもう少し一般化した結果について，文献 [38] を参照されたい．

8.8　2 次式と指標和

以下の例はベルヌーイ数にはあまり関係がないが，手法は似ている面もあるので，ついでにあげておく．ここでも p は奇素数，$\psi(x)=\left(\frac{x}{p}\right)$ は法 p の平方剰余指標とする．$P(x)$ を x の多項式とする．$\sum_{x=0}^{p-1}\psi(P(x))$ なる和を考えると，これは $y^2=P(x)$ を満たす $(x,y)\in\mathbf{F}_p$ の組の個数と関係があり，代数曲線の合同ゼータ関数と関係がある複雑な量である．一般の $P(x)$ については簡単な公式は存在しない．しかし，$P(x)$ が 2 次式であるような特別な場合は，2 次曲線に対応しているが，この場合は曲線自身の構造も単純であり，上のような和にも簡単な公式が存在する．実際にこれを計算してみよう．$P(x)=ax^2+bx+c$ $(a,b,c\in\mathbf{Z}, a\not\equiv 0 \bmod p)$ を x の 2 次多項式として和 $\sum_{x \bmod p}\psi(P(x))$ を計算するのは，それほど難しくはない．いまは p は奇素数としているから，有限体 $\mathbf{F}_p$ 内で考えて $P(x)=a((x-d)^2+e)$ と書き換えれば，

$$\sum_{x \bmod p}\psi(P(x))=\psi(a)\sum_{x \bmod p}\psi(x^2+e)$$

となり，右辺の和が本質的である．

補題 8.21 $$\sum_{x \bmod p}\psi(x^2+e)=\begin{cases}-1 & e\not\equiv 0 \bmod p \text{ のとき，}\\ p-1 & e\equiv 0 \bmod p \text{ のとき．}\end{cases}$$

証明　$\zeta=e^{2\pi i/p}$ として，

$$\psi(x^2+e)=\frac{1}{g(\psi)}\sum_{k=0}^{p-1}\psi(k)\zeta^{k(x^2+e)}$$

であった（$g(\psi)$ はガウス和）．よって

$$\sum_{x=0}^{p-1}\psi(x^2+e)=\frac{1}{g(\psi)}\sum_{k=0}^{p-1}\psi(k)\sum_{x=0}^{p-1}\zeta^{k(x^2+e)}.$$

しかし，$\sum_{x=0}^{p-1}\zeta^{kx^2}=\psi(k)g(\psi)$，また

$$\sum_{k=0}^{\infty}\psi(k)^2\zeta^{ke}=\sum_{k=1}^{p-1}\zeta^{ke}=\begin{cases}-1 & e\not\equiv 0 \bmod p\text{ のとき},\\ p-1 & e\equiv 0 \bmod p\text{ のとき}\end{cases}$$

となるので，結果を得る．■

なお，以上の結果は当然 $x^2+e=y^2$ となる $(x,y)\in\mathbf{F}_p$ の組の個数と関係がある．すなわち，各 $x\in\mathbf{F}_p$ に対してこの方程式を満たす y は $1+\psi(x^2+e)$ 個あるので，解 (x,y) の組は，$e\not\equiv 0 \bmod p$ ならば $p-1$ 組あることになる．

一般に 2 次形式 $Q(x)$（すなわち $x=(x_1,x_2,\ldots,x_n)$ の各変数 x_i についての 2 次同次式）などについて $\sum_{x \bmod p}\zeta^{Q(x)}$ などを考えることもでき，結論もよく知られているが，これはベルヌーイ数からはかなり離れるので省略する．

次に，$\sum_{x=0}^{p-1}\psi(x^2+e)x$ について考えよう．（前と違って一般の 2 次式 $P(x)$ に対する和 $\sum_{x=0}^{p-1}\psi(P(x))x$ がこれに帰着するわけではない．）ここで，

$$\begin{aligned}\sum_{x=1}^{p-1}\psi(x^2+e)x&=\sum_{x=1}^{p-1}(p-x)\psi((p-x)^2+e)\\&=\sum_{x=1}^{p-1}(p-x)\psi(x^2+e)\end{aligned}$$

より，

$$\begin{aligned}2\sum_{x=1}^{p-1}\psi(x^2+e)x&=p\sum_{x=1}^{p-1}\psi(x^2+e)\\&=p\Bigl(\sum_{x=0}^{p-1}\psi(x^2+e)-\psi(e)\Bigr)\end{aligned}$$

となる．よって，

$$\sum_{x=0}^{p-1}\psi(x^2+e)x=\begin{cases}-\frac{(1+\psi(e))p}{2} & e\not\equiv 0 \bmod p\text{ のとき},\\ \frac{p(p-1)}{2} & e\equiv 0 \bmod p\text{ のとき}\end{cases}$$

となる．

応用として，$e\notin p\mathbf{Z}$ のとき，たとえば次が成り立つことがわかる．

$$\sum_{x,y=0}^{p-1}\psi(x^2+ey^2)xy=-\frac{(1+\psi(e))p^2(p-1)}{4}.$$

証明は省略する．

8.9　2 次条件のある和

多項式 $f(x,y,z)$ に対して

$$M(f) = \{(a,b,c) \in \mathbf{Z}^3; 1 \le a,b,c \le p-1; f(a,b,c) \equiv 0 \bmod p\}$$

とおく.

命題 8.22　整数 $e \not\equiv 0 \bmod p$ に対し $h_e(x,y,z) = exz - y^2$ とすると

$$\sum_{(a,b,c)\in M(h_e)} \frac{\psi(a)}{(1-\zeta^a)(1-\zeta^b)(1-\zeta^c)} = -\frac{p-1}{4}(1+\psi(e))g(\psi)B_{1,\psi}$$

が成り立つ.

証明　左辺を I とおくと, I において, b を $-b$ で置き換えてもよいから

$$(1-\zeta^{-b})^{-1} + (1-\zeta^b)^{-1} = 1$$

より, $a\bar{a} \equiv e\bar{e} \equiv 1 \bmod p$ となる整数 $\bar{a}, \bar{e}$ をとれば,

$$\begin{aligned}
2I &= \sum_{a,b=1}^{p-1} \frac{\psi(a)}{(1-\zeta^a)(1-\zeta^{\bar{a}\bar{e}b^2})} \\
&= \sum_{a,b=1}^{p-1} \frac{\psi(a)}{(1-\zeta^a)} \left(-\frac{1}{p} \sum_{m=1}^{p-1} m\zeta^{\bar{a}\bar{e}b^2 m} \right) \\
&= -\frac{1}{p} \sum_{a,m=1}^{p-1} \frac{\psi(a)}{(1-\zeta^a)} m(\psi(\bar{a}\bar{e}m)g(\psi) - 1) \\
&= -\frac{p-1}{2}\psi(\bar{e})g(\psi)B_{1,\psi} - \frac{p-1}{2}g(\psi)B_{1,\psi} \\
&= -\frac{p-1}{2}(1+\psi(\bar{e}))g(\psi)B_{1,\psi}.
\end{aligned}$$

∎

以上の応用として次がわかる.

系 8.23

$$\sum_{(l,m,n)\in M(h_e)} \psi(n)lmn = \frac{p^3(p-1)}{4}(1+\psi(e))B_{1,\psi}.$$

証明　以下しばらく分母が p で割れない有理数 α については, ζ^α を $\alpha \in \mathbf{F}_p$ と解釈して定義するとする. すると I を前命題の証明と同様として

$$
\begin{aligned}
-p^3 I &= \sum_{l,m,n=1}^{p-1} lmn \sum_{(a,b,c)\in M(h_e)} \psi(a)\zeta^{al+bm+cn} \\
&= \sum_{l,m,n=1}^{p-1} lmn \sum_{a=1}^{p-1} \psi(a)\zeta^{al}\zeta^{-\frac{aem^2}{4n}} \sum_{b=1}^{p-1} \zeta^{\frac{n}{ae}(b+\frac{aem}{2n})^2} \\
&= \sum_{l,m,n,a=1}^{p-1} lmn\zeta^{al}\psi(a)\zeta^{-aem^2/4n}(\psi(n/(ae))g(\psi) - \zeta^{aem^2/4n}) \\
&= \sum_{l,m,n,a=1}^{p-1} lmn\zeta^{al}(\psi(ne)\zeta^{-aem^2/4n}g(\psi) - \psi(a)) \\
&= \sum_{l,m,n=1}^{p-1} (-g(\psi)\psi(ne) - \psi(l)g(\psi))lmn + pg(\psi) \sum_{4ln\equiv em^2 \bmod p} \psi(ne)lmn \\
&= -g(\psi)\left((1+\psi(e))pB_{1,\psi}\frac{p^2(p-1)^2}{4} - p \sum_{(l,m,n)\in M(h_{4/e})} \psi(ne)lmn\right).
\end{aligned}
$$

途中，$\sum_{x=0}^{p-1}\zeta^{cx^2} = \psi(c)g(\psi)$ を用いた．ここで，I の結果および右辺に e は $\psi(e)$ という形でしか現れない．そこで，$\psi(4/e) = \psi(e)$ であるので，右辺の和の条件の $M(h_{4/e})$ は $M(h_e)$ で置き換えてもよい．これより $\sum_{(l,m,n)\in M(h_e)} \psi(n)lmn$ の公式を得る． ∎

2 次条件のあるこのようなの和の一部については，概均質ベクトル空間のゼータ関数の特殊値などが関係している．しかし，一般にはよくわからないことが多い．このような指数和の公式がどういう場合に存在しうるのか，またその根拠はどこにあるのかなど，解明されていない．特別な 2 次条件については，指数和の公式について少し予想が立てられているが，証明はわかっていない．ここで取り上げるには時期尚早かと思うので予想の記述などは省略するが，一般の概均質ベクトル空間のゼータ関数の特殊値と指数和の関係という視点は解明されていない面白い問題であるかもしれない．

第 9 章

L 関数の特殊値と複素積分表示

第 4 章，5 章の続きとして，フルヴィッツゼータ関数とディリクレ L 関数の，解析接続，関数等式などの性質を調べ，負整数点での特殊値を計算する．関数等式の証明法には種々あるが，ここではコンタワー積分を用いる方法を解説する．コンタワー積分まで持ち出す必要はないという立場もあるが，それ自体面白いものであり，役にも立つので，あえてコンタワー積分と，積分路を切り開くという操作によって，関数等式を導くこととする．

9.1 フルヴィッツゼータ関数

正の実数 a に対し，ゼータ関数 $\zeta(s,a)$ を

$$\zeta(s,a) = \sum_{n=0}^{\infty} (n+a)^{-s}$$

で定義する．右辺の級数は $\mathrm{Re}(s) > 1$ で絶対収束するので，この範囲で $\zeta(s,a)$ は定義されている．$\zeta(s,a)$ はフルヴィッツゼータ関数と呼ばれる（Hurwitz [36], Whittaker[1]-Watson[2][91, Part II]）．特に $a = 1$ のとき $\zeta(s,1)$ はリーマンゼータ関数 $\zeta(s)$ にほかならない．まずこの節で，$\zeta(s,a)$ の積分表示を与えよう．

---

[1]Edmund Taylor Whittaker（1873.10.24 イギリス Southport 生——1956.3.24 イギリス Edinburgh 没）

[2]George Neville Watson（1886.1.31 イギリス Devon 生——1965.2.2 イギリス Warwickshire 没）

$\Gamma(s)$ をガンマ関数とする．$\Gamma(s)$ は $\mathrm{Re}(s)>1$ である複素数 s に対して

$$\Gamma(s)=\int_0^\infty e^{-t}t^{s-1}\,dt \tag{9.1}$$

で定義される．右辺の積分は $\mathrm{Re}(s)>0$ で絶対かつ広義一様に収束し，$\Gamma(s)$ は $\mathrm{Re}(s)>0$ で正則な関数となることがわかる．部分積分を行うことにより，ガンマ関数の最も大切な性質として，

$$\Gamma(s+1)=s\Gamma(s) \tag{9.2}$$

が得られる．等式 (9.2) を通して $\Gamma(s)$ は全 s 平面の有理型関数に解析接続される．具体的には (9.2) を

$$\Gamma(s)=\frac{\Gamma(s+1)}{s}$$

と書き直すと，右辺は $\mathrm{Re}(s)>-1$ で有理型関数となるので，まず $\Gamma(s)$ は $\mathrm{Re}(s)>-1$ に解析接続され，$s=0$ が留数 1 の 1 位の極となる．さらに，

$$\Gamma(s)=\frac{\Gamma(s+2)}{s(s+1)}$$

とし，これを繰り返して任意の自然数 M について

$$\Gamma(s)=\frac{\Gamma(s+M)}{s(s+1)\cdots(s+M-1)} \tag{9.3}$$

が成り立つ．(9.3) 式を通して $\Gamma(s)$ は $\mathrm{Re}(s)>-M$ の有理型関数に解析接続される．M は任意にとれるので，$\Gamma(s)$ は全 s 平面の有理型関数に解析接続され，$s=0,\,-1,\,-2,\cdots$ が 1 位の極になり，留数は (9.3) 式を用いて計算できる．

(9.1) 式において $t\to(n+a)t\ \ (n+a>0)$ と変数変換することにより，

$$\frac{1}{(n+a)^s}=\frac{1}{\Gamma(s)}\int_0^\infty e^{-(n+a)t}t^{s-1}\,dt$$

を得る．形式的に

$$\sum_{n=0}^\infty\frac{1}{(n+a)^s}=\frac{1}{\Gamma(s)}\int_0^\infty\sum_{n=0}^\infty e^{-(n+a)t}t^{s-1}\,dt$$

となるが，$\mathrm{Re}(s)>1$ の範囲では左辺は絶対収束するので，正しいことがわかる．したがって，$\mathrm{Re}(s)>1$ の範囲で，$\zeta(s,a)$ の積分表示

$$\zeta(s,a)=\frac{1}{\Gamma(s)}\int_0^\infty \frac{e^{-at}}{1-e^{-t}}t^{s-1}\,dt=\frac{1}{\Gamma(s)}\int_0^\infty \frac{te^{(1-a)t}}{e^t-1}t^{s-2}\,dt \qquad (9.4)$$

が得られる．この積分表示は $\zeta(s,a)$ がなにやら，ベルヌーイ多項式 $B_k(a)$ と関係がありそうだということを物語っている．

9.2 コンタワー積分

積分表示 (9.4) を複素積分の形に変形し，複素関数論の留数定理などを応用することを考えよう．積分区間 $[0,\infty)$ を複素積分の道（path）と考え，これをふくらませた次の道（積分路）$I(\varepsilon,\infty)$ $(\varepsilon>0)$ を考える．$I(\varepsilon,\infty)$ は $(-\infty,\infty)$ から $\mathbf{C}$ への写像 $\varphi:(-\infty,\infty)\longrightarrow\mathbf{C}$ として

$$I(\varepsilon,\infty): \qquad \varphi(u)=\begin{cases} -u & u<-\varepsilon, \\ \varepsilon\exp\left(\pi i\frac{u+\varepsilon}{\varepsilon}\right) & -\varepsilon\le u\le\varepsilon, \\ u & u>\varepsilon \end{cases}$$

として定義される．$I(\varepsilon,\infty)$ は定義上は，$u<-\varepsilon$ と $u>\varepsilon$ で重なっているが，$u<-\varepsilon$ では実軸の上方，$u>\varepsilon$ では実軸の下方を通ると考える．図示すると図 9.1 のようになる．

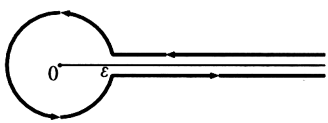


図 9.1: $I(\varepsilon,\infty)$ の図

複素線積分

$$\int_{I(\varepsilon,\infty)}\frac{te^{(1-a)t}}{e^t-1}t^{s-2}\,dt$$

を考えよう．$I(\varepsilon,\infty)$ 上で t^{s-2} を考える必要があるので，$s\in\mathbf{C}$ に対して複素数べき t^s を定義する．t の偏角を $\arg t$ とするとき，$\mathbf{C}-\{z=x+iy \mid y=0,\ x\ge 0\}$ 上の 1 価解析関数としての $\log t$ が

$$\log t=\log|t|+i\arg t \qquad (0<\arg t<2\pi)$$

で定義される．これを用いて $\mathbf{C}-\{z=x+iy \mid y=0,\ x\geq 0\}$ 上の1価解析関数 t^s は，

$$t^s=e^{s\log t}$$

で与えられる．積分路 $I(\varepsilon,\infty)$ を3つの部分

C_1: 実軸の ∞ から ε までの部分

$I(\varepsilon)$: 原点を中心とし半径 ε の円周（反時計回りにまわる）

C_2: 実軸の ε から ∞ までの部分

に分ける．$I(\varepsilon,\infty)=C_1+I(\varepsilon)+C_2$ である．t が C_1 上にあるときは $\arg t=0$, C_2 上では $\arg t=2\pi$ と考える．すると C_1 上の積分は

$$\int_{C_1}\frac{te^{(1-a)t}}{e^t-1}t^{s-2}\,dt=\int_{\infty}^{\varepsilon}\frac{te^{(1-a)t}}{e^t-1}t^{s-2}\,dt$$

$$=-\int_{\varepsilon}^{\infty}\frac{te^{(1-a)t}}{e^t-1}t^{s-2}\,dt$$

となり，C_2 上では

$$\int_{C_2}\frac{te^{(1-a)t}}{e^t-1}t^{s-2}\,dt=\int_{\varepsilon}^{\infty}\frac{te^{(1-a)t}}{e^t-1}e^{(s-2)(\log t+2\pi i)}\,dt$$

$$=e^{2\pi i(s-2)}\int_{\varepsilon}^{\infty}\frac{te^{(1-a)t}}{e^t-1}t^{s-2}\,dt$$

となる．$e^{2\pi i(s-2)}=e^{2\pi is}$ に注意してまとめると

$$\int_{I(\varepsilon,\infty)}\frac{te^{(1-a)t}}{e^t-1}t^{s-2}\,dt$$
$$=\left(e^{2\pi is}-1\right)\int_{\varepsilon}^{\infty}\frac{te^{(1-a)t}}{e^t-1}t^{s-2}\,dt+\int_{I(\varepsilon)}\frac{e^{(1-a)t}}{e^t-1}t^{s-1}\,dt \tag{9.5}$$

となる．円周 $I(\varepsilon)$ は，$t=\varepsilon e^{i\theta}$ $(0\leq\theta\leq 2\pi)$ と助変数表示されるので，$I(\varepsilon)$ 上では $t^{s-1}=\varepsilon^{s-1}e^{i(s-1)\theta}$ となり，積分の絶対値は

$$\left|\int_{I(\varepsilon)}\frac{e^{(1-a)t}}{e^t-1}t^{s-1}\,dt\right|\leq\int_0^{2\pi}\left|\frac{e^{(1-a)\varepsilon e^{i\theta}}}{e^{\varepsilon e^{i\theta}}-1}\varepsilon^{s-1}e^{i(s-1)\theta}i\varepsilon e^{i\theta}\right|\,d\theta \tag{9.6}$$

$$=\varepsilon^{\mathrm{Re}(s)}\int_0^{2\pi}\left|\frac{e^{(1-a)\varepsilon e^{i\theta}}}{e^{\varepsilon e^{i\theta}}-1}e^{is\theta}\right|\,d\theta$$

のように変形される．$\frac{\varepsilon}{e^{\varepsilon e^{i\theta}}-1}$ は ε と θ について有界なので，$\varepsilon \to 0$ とすれば，$\mathrm{Re}(s) > 1$ ならば (9.6) 式により

$$\lim_{\varepsilon \to 0} \int_{I(\varepsilon)} \frac{e^{(1-a)t}}{e^t - 1} t^{s-1}\, dt = 0 \tag{9.7}$$

である．一方，(9.5) 式において，関数論のコーシーの積分定理により，左辺の線積分は十分小である正数 ε ($\varepsilon < 2\pi$) の取り方によらない．なぜなら別の $\varepsilon' > 0$ をとるとき，2 つの道に囲まれる領域において被積分関数は 1 価正則になるからである．さて $\mathrm{Re}(s) > 1$ としよう．(9.5) 式において，左辺は $\varepsilon > 0$ によらないので，左辺の ε は止めておいて，右辺において $\varepsilon \to 0$ とする．このとき (9.7) 式を用いて

$$\int_{I(\varepsilon,\infty)} \frac{te^{(1-a)t}}{e^t - 1} t^{s-2}\, dt = \left(e^{2\pi i s} - 1\right) \int_0^\infty \frac{te^{(1-a)t}}{e^t - 1} t^{s-2}\, dt \tag{9.8}$$

を得る．これより，$\zeta(s,a)$ の次なる線積分表示を得る．

命題 9.1 ε を正数 ($\varepsilon < 2\pi$) とする．$\mathrm{Re}(s) > 1$ ならば，フルヴィッツゼータ関数 $\zeta(s,a)$ ($a > 0$) はコンタワー積分表示

$$\zeta(s,a) = \frac{1}{\Gamma(s)(e^{2\pi i s} - 1)} \int_{I(\varepsilon,\infty)} \frac{te^{(1-a)t}}{e^t - 1} t^{s-2}\, dt$$

をもつ．この公式を通して，$\zeta(s,a)$ は全 s 平面の有理型関数に解析接続され，極は $s = 1$ のみの 1 位の極で留数は 1 である．

証明 前半部は $\zeta(s,a)$ の積分表示 (9.4) と (9.8) より直ちに得られる．後半部は以下に順に示すことにする．

準備の補題として，

補題 9.2 積分 $\displaystyle\int_{I(\varepsilon,\infty)} \frac{te^{(1-a)t}}{e^t - 1} t^{s-2}\, dt$ は任意の $s \in \mathbf{C}$ に対し絶対収束し，全 s 平面の正則関数を表す．

証明 線積分 $\displaystyle\int_{C_j} \frac{te^{(1-a)t}}{e^t - 1} t^{s-2}\, dt$ ($j = 1,\ 2$) は任意の $s \in \mathbf{C}$ に対し絶対収束し，そこで正則になる．線積分 $\displaystyle\int_{I(\varepsilon)} \frac{te^{(1-a)t}}{e^t - 1} t^{s-2}\, dt$ についても，$\varepsilon > 0$ は固定されているので，(9.6) 式により，任意の s について絶対収束し，s について微分可能なので，全 s 平面の正則関数になる． ∎

関数論で知られるように $\dfrac{1}{\Gamma(s)}$ は全 s 平面の正則関数になるので，命題 9.1 と補題 9.2 により，$\zeta(s,a)$ の極は関数 $(e^{2\pi is}-1)$ の零点に由来する．$\zeta(s,a)$ は $\mathrm{Re}(s)>1$ では絶対収束し正則になるので，極の可能性のある点は $s=1$ および $s=1-m$ $(m\in\mathbf{N})$ である．このうち，$s=1-m$ では，関数

$$\frac{1}{\Gamma(s)(e^{2\pi is}-1)}$$

は正則になるので，$\zeta(s,a)$ の極は $s=1$ のみで 1 位の極となり，留数は

$$\begin{aligned}
&\lim_{s\to1}\frac{(s-1)}{\Gamma(s)(e^{2\pi is}-1)}\int_{I(\varepsilon,\infty)}\frac{te^{(1-a)t}}{e^t-1}t^{s-2}\,dt\\
&=\frac{1}{2\pi i}\int_{I(\varepsilon,\infty)}\frac{te^{(1-a)t}}{e^t-1}t^{-1}\,dt\\
&=\frac{1}{2\pi i}\int_{I(\varepsilon)}\frac{te^{(1-a)t}}{e^t-1}t^{-1}\,dt=\operatorname*{Res}_{t=0}\left(\frac{e^{(1-a)t}}{e^t-1}\right)=1.
\end{aligned}$$

最後の積分計算も留数計算による．$I(\varepsilon)$ の内部に含まれる被積分関数 $\dfrac{e^{(1-a)t}}{e^t-1}$ の極は $t=0$ のみで，1 位の極だからそこでの留数を計算すればよい．

これで命題 9.1 の後半部の証明が完成した．　■

次に $\zeta(s,a)$ の非正整数点 $s=1-m$ $(m\in\mathbf{N})$ での特殊値をコンタワー積分表示を利用して計算しよう．

命題 9.3　m を自然数とするとき

$$\zeta(1-m,a)=-\frac{B_m(a)}{m}.$$

ここに $B_m(a)$ は 4.3 節（55 ページ）で定義したベルヌーイ多項式である．

証明　命題 9.1 により

$$\zeta(1-m,a)=\left(\lim_{s\to1-m}\frac{1}{\Gamma(s)(e^{2\pi is}-1)}\right)\int_{I(\varepsilon,\infty)}\frac{te^{(1-a)t}}{e^t-1}t^{-m-1}\,dt.$$

最後の線積分において，被積分関数 $\frac{te^{(1-a)t}}{e^t-1}t^{-m-1}$ は $\mathbf{C}\setminus\{0\}$ で 1 価正則になる．先の記号を使うと，$I(\varepsilon,\infty)=C_1+I(\varepsilon)+C_2$ において，C_1, C_2 上の線積分は消しあう．すなわち，

$$\int_{C_1}\frac{te^{(1-a)t}}{e^t-1}t^{-m-1}\,dt+\int_{C_2}\frac{te^{(1-a)t}}{e^t-1}t^{-m-1}\,dt=0.$$

$I(\varepsilon)$ 上の線積分の計算は留数計算による．被積分関数 $\frac{te^{(1-a)t}}{e^t-1}t^{-m-1}$ の $t=0$ での留数は，ベルヌーイ多項式についての命題 4.9 の (5) と (4) より

$$\operatorname*{Res}_{t=0}\left(\frac{te^{(1-a)t}}{e^t-1}t^{-m-1}\right)=\frac{B_m(1-a)}{m!}=(-1)^m\frac{B_m(a)}{m!}.$$

一方，極限の計算は (9.3) 式により

$$\begin{aligned}\lim_{s\to 1-m}\frac{1}{\Gamma(s)(e^{2\pi is}-1)}&=\lim_{s\to 1-m}\frac{s(s+1)\cdots(s+m-1)}{\Gamma(s+m)\left(e^{2\pi i(s+m-1)}-1\right)}\\&=\frac{(-1)(-2)\cdots(1-m)}{2\pi i}\\&=\frac{(-1)^{m-1}(m-1)!}{2\pi i}\end{aligned}$$

となるので，

$$\zeta(1-m,a)=(-1)^{m-1}(m-1)!\operatorname*{Res}_{t=0}\left(\frac{te^{(1-a)t}}{e^t-1}t^{-m-1}\right).$$

これより，命題 9.3 は導かれる． ∎

9.3 $\zeta(s,a)$ の関数等式

いま $t_0<0$ とし，t 平面において $C(t_0)$ を $\mathrm{Re}(t)=t_0$ で表される上向きの直線とする．すなわち

$$C(t_0): t=t_0+iy \qquad (-\infty<y<\infty).$$

$\mathrm{Re}(s)<0$ とする．フルヴィッツゼータ関数 $\zeta(s,a)$ のコンタワー積分表示（命題 9.1）において，積分路 $I(\varepsilon,\infty)$ を図 9.2 のように切り開いて，虚軸を通り越して直線 $-C(t_0)$ までシフトする．ここでは $0<a\le 1$ とする．

虚軸を通り越すとき，被積分関数 $\dfrac{te^{(1-a)t}}{e^t-1}t^{s-2}$ の極 $t=2\pi in$ ($n\in\mathbf{Z}$, $n\neq 0$) を通るので，そこでの留数が現れる．$\mathrm{Re}(s)<0$ と $0<a\le 1$ は積分が収束するための条件である．$0<a\le 1$ の条件下では $C(t_0)$ に沿う線積分は絶対収束する．

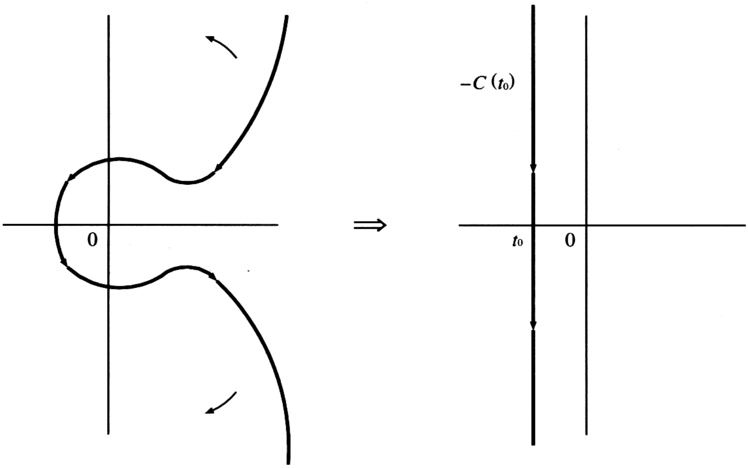


図 9.2: 積分路のシフト

$$\zeta(s,a)=\frac{1}{\Gamma(s)(e^{2\pi is}-1)}\left\{(-2\pi i)\sum_{\substack{n\in\mathbf{Z}\\ n\neq 0}}\frac{e^{(1-a)2\pi in}}{(2\pi in)^{1-s}}-\int_{C(t_0)}\frac{te^{(1-a)t}}{e^t-1}t^{s-2}\,dt\right\}$$

$$=\frac{1}{\Gamma(s)(e^{2\pi is}-1)}\left\{(-2\pi i)\sum_{n=1}^{\infty}\frac{e^{-2\pi ina}e^{\frac{\pi i}{2}(s-1)}+e^{2\pi ina}e^{\frac{3\pi i}{2}(s-1)}}{(2\pi n)^{1-s}}\right.$$

$$\left.-\int_{C(t_0)}\frac{te^{(1-a)t}}{e^t-1}t^{s-2}\,dt\right\}$$

と変形されるから，$t_0\longrightarrow-\infty$ の極限をとって，

$$\zeta(s,a)=\frac{(-\pi i)(2\pi)^{s-1}}{\Gamma(s)\sin\pi s}\left\{e^{\frac{\pi is}{2}}\sum_{n=1}^{\infty}\frac{e^{2\pi ina}}{n^{1-s}}-e^{-\frac{\pi is}{2}}\sum_{n=1}^{\infty}\frac{e^{-2\pi ina}}{n^{1-s}}\right\}\tag{9.9}$$

となる．ここで a を $1-\{a\}$ にかえて

$$\zeta(s,1-\{a\})=\frac{(-\pi i)(2\pi)^{s-1}}{\Gamma(s)\sin\pi s}\left\{e^{\frac{\pi is}{2}}\sum_{n=1}^{\infty}\frac{e^{-2\pi ina}}{n^{1-s}}-e^{-\frac{\pi is}{2}}\sum_{n=1}^{\infty}\frac{e^{2\pi ina}}{n^{1-s}}\right\}\tag{9.10}$$

が得られる．記号 $\{a\}$ は $0\le\{a\}<1$, $a-\{a\}\in\mathbf{Z}$ なる実数を表す．この変形は $\mathrm{Re}(s)<0$ で許される．これらの式 (9.9)，(9.10) より

$$e^{\frac{\pi i s}{2}}\zeta(s,a)+e^{-\frac{\pi i s}{2}}\zeta(s,1-\{a\})=\frac{(2\pi)^s}{\Gamma(s)}\sum_{n=1}^{\infty}\frac{e^{2\pi i n a}}{n^{1-s}} \tag{9.11}$$

が得られ，$\zeta(s,a)$ は全 s 平面の有理型関数に解析接続されるので，$\displaystyle\sum_{n=1}^{\infty}\frac{e^{2\pi i n a}}{n^{1-s}}$ も有理型関数に解析接続される．まとめると，次の定理になる．

定理 9.4 $0<a\leq 1$ とする．フルヴィッツゼータ関数 $\zeta(s,a)$ は全 s 平面の有理型関数に解析接続され，極は $s=1$ のみの 1 位の極で，留数は 1 である．さらに関数等式

$$\zeta(s,a)=\frac{(-\pi i)(2\pi)^{s-1}}{\Gamma(s)\sin\pi s}\left\{e^{\frac{\pi i s}{2}}\sum_{n=1}^{\infty}\frac{e^{2\pi i n a}}{n^{1-s}}-e^{-\frac{\pi i s}{2}}\sum_{n=1}^{\infty}\frac{e^{-2\pi i n a}}{n^{1-s}}\right\}$$

を満たす．

ここで $s=1-m$ とおいて 59 ページの (4.3) 式を使うと先の命題 9.3 が得られる．

また，(9.11) 式において $a=1$ とすると $\zeta(s,1)=\zeta(s)$ に注意して

$$\zeta(s)=\frac{(2\pi)^s}{2\Gamma(s)\cos\frac{\pi s}{2}}\cdot\zeta(1-s)=\frac{(2\pi)^s}{2\Gamma(s)\sin\frac{\pi(s+1)}{2}}\cdot\zeta(1-s)$$

が得られる．そこで，ガンマ関数の倍角の公式

$$\Gamma(s)=\pi^{-1/2}2^{s-1}\Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{s+1}{2}\right)$$

とガンマ関数と三角関数とを結びつける公式（ガンマ関数の相補公式）

$$\Gamma(s)\Gamma(1-s)=\frac{\pi}{\sin\pi s}$$

（これらの公式については，たとえば [91, 第 11 章]，[81, 第 7 章] など参照）を用いると

$$\Gamma\left(\frac{s}{2}\right)\zeta(s)=\pi^{1/2}2^{1-s}\frac{(2\pi)^s}{2\Gamma\left(\frac{s+1}{2}\right)\sin\frac{\pi(s+1)}{2}}\zeta(1-s)$$

$$=\pi^{s-1/2}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s)$$

となる．整形すると，リーマンゼータ関数の関数等式になる．

定理 9.5（リーマンゼータ関数の関数等式） リーマンゼータ関数 $\zeta(s)$ は，全

s 平面の有理型関数に解析接続され，

$$\xi(s) = \pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s)$$

とおくと関数等式

$$\xi(s) = \xi(1-s)$$

を満たす．

9.4　L 関数の特殊値と関数等式

この節ではディリクレ L 関数を定義し，その関数等式や整数点での特殊値を求めることを目標としよう．

χ を f を法とするディリクレ指標とする．指標 χ つきのディリクレ L 関数は

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

で定義され，右辺の級数は $\mathrm{Re}(s) > 1$ で絶対収束し，その範囲での正則関数になる．

まず，正の整数点での特殊値を考えてみよう．

χ に付随したガウス和 $g(\chi)$ は

$$g(\chi) = \sum_{a=1}^{f} \chi(a)e^{2\pi ia/f}$$

で定義された（110 ページ定義 8.1）．χ を f を法とする原始的指標とするとき，補題 8.2 より任意の整数 n に対して

$$\chi(n)g(\overline{\chi}) = \sum_{a=1}^{f} \overline{\chi}(a)e^{2\pi ian/f} \tag{9.12}$$

が成り立つ．

定理 9.6　χ を f を法とする原始的指標とし，k は自然数とする．$\chi(-1) = (-1)^k$ であれば，ディリクレ L 関数 $L(s,\chi)$ の $s = k$ での特殊値は

$$L(k,\chi) = \frac{(-1)^{k-1}(2\pi i)^k}{2\cdot k!f^k}g(\chi)B_{k,\overline{\chi}}$$

で与えられる．

先に例を挙げよう．

例 9.7 χ を 4 を法とする原始的指標，k を正の奇数とすると，$\overline{\chi}=\chi$, $g(\chi)=2i$ であるので，

$$L(k,\chi)=\frac{(-1)^{\frac{k+1}{2}}\pi^k}{2^k k!}B_{k,\chi}.$$

具体的に 2 つばかり書くと，4.2 節の表示により $B_{1,\chi}=-\frac{1}{2}$, $B_{3,\chi}=\frac{3}{2}$ なので，

$$L(1,\chi)=1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+\cdots=\frac{\pi}{4},$$

$$L(3,\chi)=1-\frac{1}{3^3}+\frac{1}{5^3}-\frac{1}{7^3}+\cdots=\frac{\pi^3}{32}.$$

次に χ を 3 を法とする原始的指標とする．$B_{1,\chi}=-\frac{1}{3}$, $B_{3,\chi}=\frac{2}{3}$, $g(\chi)=\sqrt{3}i$ であるので，

$$L(1,\chi)=1-\frac{1}{2}+\frac{1}{4}-\frac{1}{5}+\frac{1}{7}-\frac{1}{8}+\cdots=\frac{\pi}{3\sqrt{3}},$$

$$L(3,\chi)=1-\frac{1}{2^3}+\frac{1}{4^3}-\frac{1}{5^3}+\frac{1}{7^3}-\frac{1}{8^3}+\cdots=\frac{2^2\pi^3}{3^4\sqrt{3}}.$$

証明 (9.12) 式を用いると

$$L(k,\chi)g(\overline{\chi})=\sum_{a=1}^{f}\overline{\chi}(a)\sum_{n=1}^{\infty}\frac{e^{2\pi ian/f}}{n^k}$$

となり，仮定の $\chi(-1)=(-1)^k$ に注意すると右辺は，

$$\frac{1}{2}\sum_{a=1}^{f}\overline{\chi}(a)\sum_{\substack{n\in\mathbf{Z}\\ n\neq 0}}\frac{e^{2\pi ian/f}}{n^k}$$

と変形される．定理 4.11（59 ページ）と 54 ページの (4.1) 式によりこの値は

$$\frac{-(2\pi i)^k}{2k!}\sum_{a=1}^{f}\overline{\chi}(a)B_k(a/f)=\frac{-(2\pi i)^k}{2k!f^{k-1}}B_{k,\overline{\chi}}$$

と書き換えられる．前章補題 8.2，8.3 より $g(\overline{\chi})^{-1}=\chi(-1)g(\chi)/f$ に注意すれば，これより定理が導かれる． ∎

$L(s,\chi)$ をフルヴィッツゼータ関数を用いて表そう．L 関数の種々の性質を導き出すのにフルヴィッツゼータ関数は大変有用である．$\mathrm{Re}(s)>1$ の条件下で

$$L(s,\chi)=\sum_{a=1}^{f}\sum_{m=0}^{\infty}\frac{\chi(a+fm)}{(a+fm)^s}$$

$$=\sum_{a=1}^{f}\chi(a)\sum_{m=0}^{\infty}\frac{1}{(a+fm)^s}$$

$$=f^{-s}\sum_{a=1}^{f}\chi(a)\sum_{m=0}^{\infty}\frac{1}{(m+a/f)^s}$$

と変形され，次の命題が従う．

命題 9.8 χ を f を法とする原始的ディリクレ指標とする．このとき，$\mathrm{Re}(s)>1$ の範囲で

$$L(s,\chi)=f^{-s}\sum_{a=1}^{f}\chi(a)\zeta(s,\frac{a}{f}).$$

$L(s,\chi)$ はこの表示式を通して全 s 平面で正則な関数に解析接続される．

証明 前半部はすでに示した．後半部は命題 9.1 を用いる．命題 9.1 により，フルヴィッツゼータ関数 $\zeta(s,a/f)$ は全 s 平面の有理型関数に解析接続され，極は $s=1$ のみで 1 位の極である．したがって，$L(s,\chi)$ は全 s 平面の有理型関数に解析接続され，極はあるとしても $s=1$ のみで 1 位の極である．$s=1$ での留数を計算すると

$$f^{-1}\sum_{a=1}^{f}\chi(a)=0$$

となり，$s=1$ でも正則なことがわかる． ∎

$L(s,\chi)$ の関数等式をフルヴィッツゼータ関数の関数等式（定理 9.4）から導こう．記号 $\delta=\delta(\chi)$ を

$$\delta=\begin{cases}0 & \chi(-1)=1\text{ のとき},\\ 1 & \chi(-1)=-1\text{ のとき}\end{cases}$$

とおく．

定理 9.9（関数等式） χ は f を法とする原始的指標とする．このとき，$L(s,\chi)$ は関数等式

$$\left(\frac{f}{\pi}\right)^{s/2}\Gamma\left(\frac{s+\delta}{2}\right)L(s,\chi)=W(\chi)\left(\frac{f}{\pi}\right)^{(1-s)/2}\Gamma\left(\frac{1-s+\delta}{2}\right)L(1-s,\overline{\chi})$$

を満たす．ただし，

$$W(\chi)=\frac{g(\chi)}{\sqrt{f}i^{\delta}}$$

とした．

証明　命題 9.8 と定理 9.4 により，$\mathrm{Re}(s)<0$ まで解析接続して考えて，

$$L(s,\chi)=f^{-s}\sum_{a=1}^{f}\chi(a)\zeta(s,\frac{a}{f})$$

$$=\frac{(-\pi i)(2\pi)^{s-1}}{f^s\Gamma(s)\sin\pi s}\left\{e^{\frac{\pi is}{2}}\sum_{n=1}^{\infty}\sum_{a=1}^{f}\frac{\chi(a)e^{2\pi in\frac{a}{f}}}{n^{1-s}}-e^{\frac{-\pi is}{2}}\sum_{n=1}^{\infty}\sum_{a=1}^{f}\frac{\chi(a)e^{-2\pi in\frac{a}{f}}}{n^{1-s}}\right\}$$

となる．ここで (9.12) 式を用いると

$$L(s,\chi)=\frac{(-\pi i)(2\pi)^{s-1}g(\chi)}{f^s\Gamma(s)\sin\pi s}\left(e^{\frac{\pi is}{2}}-\chi(-1)e^{\frac{-\pi is}{2}}\right)L(1-s,\overline{\chi})$$

を得る．整理すると

$$\Gamma(s)\cos\left(\frac{\pi(s-\delta)}{2}\right)L(s,\chi)=\frac{g(\chi)}{2i^{\delta}}\left(\frac{2\pi}{f}\right)^{s}L(1-s,\overline{\chi}) \tag{9.13}$$

となる．$\Gamma(s)$ の倍角の公式と $\Gamma(s)\Gamma(1-s)=\dfrac{\pi}{\sin\pi s}$ を使って

$$\Gamma(s)=\pi^{-1/2}2^{s-1}\Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{s+1}{2}\right)$$

$$=\pi^{-1/2}2^{s-1}\Gamma\left(\frac{s+\delta}{2}\right)\frac{\pi}{\Gamma\left(\frac{1-s+\delta}{2}\right)\cos\frac{\pi(s-\delta)}{2}}$$

の形に書き直して (9.13) 式に代入整理すると求める関数等式になる．∎

最後に $L(s,\chi)$ の負整数点での特殊値を求めよう．

定理 9.10　χ を f を法とする原始的指標とする．m を正整数とするとき，

$$L(1-m,\chi)=-\frac{B_{m,\chi}}{m}$$

で与えられる．

証明　命題 9.8 と命題 9.3 により，

$$L(1-m,\chi) = f^{m-1}\sum_{a=1}^{f}\chi(a)\zeta\left(1-m,\frac{a}{f}\right)$$

$$= -f^{m-1}\sum_{a=1}^{f}\chi(a)\frac{B_m(a/f)}{m}.$$

54 ページ (4.1) 式よりこれは $-\frac{B_{m,\chi}}{m}$ と等しい．■

注意 9.11　定理 9.6 は定理 9.10 と関数等式（定理 9.9）からも導かれることに注意する．

第10章

類数公式とやさしい概均質ベクトル空間のゼータ関数

この章では，2次形式と2次体の対応の応用として，2次形式で決まる簡単な概均質ベクトル空間のゼータ関数を具体的に表示することを考える．その前に，前に述べた2次形式の理論では，やや足りない部分があるので2次体のイデアルの乗法構造についての説明を補足する．

10.1 2次体のイデアル群

この節の内容については，詳しくは，Lang [60]，高木 [80]，Weber[1][89] などを参照されたい．2次形式との関係で第6章でイデアルの説明をしたときに，イデアルの積の構造にはあえて触れなかった．しかしやはりイデアルの群の構造は重要なので，これをここで説明したい．

群と見なすには，逆元が必要なので，分数イデアルという，$\mathfrak{O}_f$ には含まれない加群を考える必要が生じる．これを導入する準備として，まず2次体 $K=\mathbf{Q}(\sqrt{m})$ の自由部分加群 L を考える．L の自由加群としての階数は高々2である．これは次のようにしてわかる．L の階数を n として $\mathbf{Z}$ 上の基底を $\omega_i=a_i+b_i\sqrt{m}$ (a_i, $b_i\in\mathbf{Q}$, $1\leq i\leq n$) とおく．十分大きな整数 r をとり ra_i, $rb_i\in\mathbf{Z}$ ($1\leq i\leq n$) としておいてよい．当然 $r\omega_i$ ($1\leq i\leq n$) が $\mathbf{Z}$ 上生成する加群 rL も階数 n の自由加群になるが，$r\omega_i\in\mathbf{Z}+\mathbf{Z}\sqrt{m}$ であるから $rL\subset\mathbf{Z}+\mathbf{Z}\sqrt{m}$ である．$\mathbf{Z}+\mathbf{Z}\sqrt{m}$

[1]Heinrich Martin Weber（1842.5.5 ドイツ Heidelberg 生——1913.5.17 フランス Strassbourg 没）

は階数 2 の自由加群であるから，アーベル群の基本定理により rL，したがって L の階数も 2 以下である．

定義 10.1　2 次体 $K = \mathbf{Q}(\sqrt{m})$ の階数が 2 の自由加群を K の格子（lattice）という．

格子 L_1，L_2 について，積を

$$L_1L_2 = \{\sum_{i=1}^{\nu} a_ib_i;\ a_i \in L_1,\ b_i \in L_2,\ \nu \text{ は任意の自然数}\}$$

で定義する．積もまた格子になる．実際，前と同様 $rL_1, rL_2 \subset \mathbf{Z} + \mathbf{Z}\sqrt{m}$ となる r が存在するが，$\mathbf{Z} + \mathbf{Z}\sqrt{m}$ は明らかに環だから，$r^2L_1L_2 \subset \mathbf{Z} + \mathbf{Z}\sqrt{m}$ となり，L_1L_2 も自由加群である．階数が 2 であることは，$0 \neq \omega \in L_1$ について $\omega L_2 \subset L_1L_2$ で，ωL_2 が階数 2 であるから明らかである．

さて，整環 $\mathfrak{O}_f$ のイデアルの群構造を考えるためには，逆元に当たるものがなければならない．$\mathfrak{a}$ について，$\mathfrak{a}L = \mathfrak{O}_f$ となる格子 L を考えたい．しかし，一般にはこのような格子は存在するとは限らない．

例 10.2　$K = \mathbf{Q}(\sqrt{-2})$ とし，導手が 5 の整環 $\mathfrak{O}_5 = \mathbf{Z} + 5\sqrt{-2}\mathbf{Z}$ を考える．$\mathfrak{a} = 5\mathbf{Z}+5\sqrt{-2}\mathbf{Z}$ とおくと，これは $\mathfrak{O}_f$ のイデアルであるが $\mathfrak{a}L = \mathfrak{O}_5$ となる格子 L は存在しない．なぜなら，もし存在すれば，$5L \subset \mathfrak{O}_5$ より，L の任意の元 α は $\alpha = a/5 + b\sqrt{-2}$ $(a, b \in \mathbf{Z})$ と書けるが $(5\sqrt{-2})\alpha = (-10b) + a\sqrt{-2} \in \mathfrak{O}_5$ より，$a \in 5\mathbf{Z}$ となる．よって $L \subset \mathbf{Z}+\mathbf{Z}\sqrt{-2}$ となり，ゆえに $\mathfrak{a}L \subset 5(\mathbf{Z}+\mathbf{Z}\sqrt{-2}) \neq \mathfrak{O}_5$ となる．

補題 10.3　$\mathfrak{a}$ が $\mathfrak{O}_f$ の固有イデアルならば $\mathfrak{a}L = \mathfrak{O}_f$ となる K の格子 L で $\mathfrak{O}_f$ 加群になるものが存在してただ 1 つである．

証明　まず，このような L を 1 つ具体的に与える．$\mathfrak{a}$ が原始的イデアルのときに与えれば十分である．1，ω を極大整環の標準的な基底とし，$\mathfrak{a} = \mathbf{Z}a + \mathbf{Z}(d + f\omega)$ と標準基底で表示しておく．$x \mapsto \overline{x}$ を $K/\mathbf{Q}$ の自明でない同型写像として，$M = \mathbf{Z} + \mathbf{Z}a^{-1}(d + f\overline{\omega})$ とおく．これは明らかに $\mathfrak{O}_f$ 加群である．積をとると，

$$\mathfrak{a}M = \mathbf{Z}a + \mathbf{Z}(d + f\omega) + \mathbf{Z}(d + f\overline{\omega}) + \mathbf{Z}a^{-1}(d + f\omega)(d + f\overline{\omega})$$

となる．ここで，$\mathfrak{a}$ がイデアルであることより，$c := a^{-1}(d + f\omega)(d + f\overline{\omega})$ は整数である（80 ページ補題 6.4）．また，$\mathfrak{a}$ が固有イデアルという条件から，a，$b := 2d + fTr(\omega)$，c は互いに素であった（81 ページ補題 6.5）．しかし，上の

式から $a,b,c \in \mathfrak{a}M$ であるから，$1 \in \mathfrak{a}M$ となる．よって $d + f\omega \in \mathfrak{a}M$ より $f\omega \in \mathfrak{a}M$ となって，$\mathfrak{O}_f \subset \mathfrak{a}M$ がわかる．$\mathfrak{a}M \subset \mathfrak{O}_f$ は明らかであるから，前半は証明された．ただ 1 つしか存在しないことを示す．L を $\mathfrak{O}_f$ 加群となる格子とし，$\mathfrak{a}L = \mathfrak{O}_f$ とする．

$$N = \{\mu \in K;\ \mu\mathfrak{a} \subset \mathfrak{O}_f\}$$

とおくと，N は明らかに $\mathfrak{O}_f$ 加群であり，$L \subset N$ は明らかである．$\mu \in N$ とすると $\mu\mathfrak{a}L \subset \mathfrak{O}_f L$ であるが，L は $\mathfrak{O}_f$ 加群と仮定しているから，$\mathfrak{O}_f L \subset L$ であり，$1 \in \mathfrak{O}_f$ より，$\mathfrak{O}_f L = L$ である．一方，$\mathfrak{a}L = \mathfrak{O}_f$ であるから，$\mu\mathfrak{O}_f \subset L$ となる．よって，$\mu \in L$ である．すなわち $L = N$ が示された．∎

上で定義した M を $\mathfrak{a}^{-1}$ と書き，$\mathfrak{a}$ の逆イデアルと呼ぶ．固有イデアルの概念を少し拡張して，K の格子 L が

$$\{\lambda \in K; \lambda L \subset L\} = \mathfrak{O}_f$$

となるとき，L を $\mathfrak{O}_f$ の固有分数イデアルということにする．（単にイデアルという場合は必ず $\mathfrak{O}_f$ の部分集合となるもののこととする．）$\mathfrak{O}_f$ の固有イデアル $\mathfrak{a}$ に対して $\mathfrak{a}^{-1}$ は固有分数イデアルである．真の固有分数イデアル L は，適当な整数 r をかけると $rL \subset \mathfrak{O}_f$ となり，rL は明らかに $\mathfrak{O}_f$ の固有イデアルであるから L も逆イデアルをもつ．

補題 10.4　$\mathfrak{O}_f$ の固有分数イデアル L_1 と L_2 の積 L_1L_2 は固有分数イデアルである．

証明　イデアルについて証明すれば十分である．$\mathfrak{a}$，$\mathfrak{b}$ を固有イデアルとして，$\mathfrak{ab} = \mathfrak{c}$ とする．$\alpha \in K$ について $\alpha\mathfrak{c} \subset \mathfrak{c}$ とする．$\mathfrak{a}$ が固有イデアルだから $\mathfrak{a}^{-1}$ が存在し，$\mathfrak{a}^{-1}\mathfrak{c} = \mathfrak{a}^{-1}\mathfrak{ab} = \mathfrak{b}$ である．よって，$\alpha\mathfrak{b} \subset \mathfrak{b}$ となり，$\mathfrak{b}$ が固有イデアルだから $\alpha \in \mathfrak{O}_f$ となる．∎

以上をまとめて次を得る．

命題 10.5　$\mathfrak{O}_f$ の固有分数イデアル全体は $\mathfrak{O}_f$ を単位元とする群をなす．

このようにして定義された群を $\mathfrak{O}_f$ のイデアル群という．分数イデアルでもイデアルの同値は普通のイデアルと同様に定義され，この同値類で割った群をイデアル類群という．$\mathfrak{O}_f$ の類数とは，つまりは $\mathfrak{O}_f$ のイデアル類群の位数である．

$\mathfrak{O}_{\max}$ のイデアル群に比べると，f が一般の場合は，少し取り扱いが面倒な

イデアルが存在する．しかし，2次形式のところでも見たように，実際にはイデアルの同値類が問題になることが多く，面倒なイデアルは避けて，同値類の個数は減らないようにイデアル群の部分群をとることができる．これを次に説明する．

定義 10.6　$\mathfrak{O}_f$ のイデアル $\mathfrak{a}$ で

$$\mathfrak{a} + f\mathfrak{O}_f = \mathfrak{O}_f$$

となるものを f と素なイデアルという．

補題 10.7　$\mathfrak{a}$ が f と素であるための必要十分条件は $\mathfrak{a}$ のノルムが f と素なことである．また f と素なイデアルはいつでも固有イデアルになる．

証明　$\mathfrak{a} = l\mathfrak{b}$ で $\mathfrak{b}$ は原始的としておく．標準基底をとって $\mathfrak{b} = \mathbf{Z}a + \mathbf{Z}(d + f\omega)$ とおく．$N(\mathfrak{a}) = al^2$ であった．$\mathfrak{a} + f\mathfrak{O}_f$ は明らかに $\mathfrak{O}_f$ のイデアルであるから $\mathfrak{a}$ が f と素であるための必要十分条件は，$1 \in \mathfrak{a} + f\mathfrak{O}_f$，つまり

$$l(xa + y(d + f\omega)) + f(z + wf\omega) = 1$$

となる $x,y,z,w \in \mathbf{Z}$ が存在することである．これはつまり $lxa + lyd + zf = 1$, $lyf + wf^2 = 0$ である．このような x, y, z, w が存在したとすると，第2式より ly が f で割れ，すると第1式より $(f, la) = 1$ でなければならない．すなわち $(f, N(\mathfrak{a})) = 1$．逆に $(f, la) = 1$ とすると，$lax + ft = 1$ となる x, t が存在し，t を ld で割って $t = z + ldy'$ と書き，$y = fy', w = -ly'$ とおくと上記を満たす x, y, z, w を得る．$f\mathfrak{O}_{\max} \subset \mathfrak{O}_f$ であるから f と素なイデアルについては

$$\mathfrak{a} + f\mathfrak{O}_f \subset \mathfrak{a} + f\mathfrak{O}_{\max} \subset \mathfrak{O}_f$$

より，$\mathfrak{a} + f\mathfrak{O}_{\max} = \mathfrak{O}_f$ でもある．$\alpha\mathfrak{a} \subset \mathfrak{a}$ ならば $\alpha \in \mathfrak{O}_{\max}$ であるから，

$$\alpha\mathfrak{O}_f \subset \alpha\mathfrak{a} + f\alpha\mathfrak{O}_{\max} \subset \mathfrak{O}_f$$

となる．よって $\mathfrak{a}$ は固有イデアルである．　■

$\mathfrak{O}_f$ のイデアルの中で f と素なもの全体を $I(\mathfrak{O}_f, f)$ と書くことにする．また，$\mathfrak{O}_{\max}$ のイデアルでノルムが f と素なもの全体を $I(\mathfrak{O}_{\max}, f)$ と書く．

補題 10.8　写像 $I(\mathfrak{O}_{\max}, f) \to I(\mathfrak{O}_f, f)$ を $\mathfrak{a} \to \mathfrak{a} \cap \mathfrak{O}_f$ と定義すると，これは全単射であり，積を積に写す．また，この写像はノルムを保つ．

証明　まずノルムを保つことを示す．$\mathfrak{a} \in I(\mathfrak{O}_{\max}, f)$ とすれば 環の同型定理より，

$$\mathfrak{O}_f/\mathfrak{a} \cap \mathfrak{O}_f \cong (\mathfrak{O}_f + \mathfrak{a})/\mathfrak{a}.$$

ここで，$\mathfrak{a}$ は f と素なのであるから $\mathfrak{a}+f\mathfrak{O}_{\max}=\mathfrak{O}_{\max}$ であるが，$f\mathfrak{O}_{\max}\subset\mathfrak{O}_f$ より $\mathfrak{O}_f+\mathfrak{a}=\mathfrak{O}_{\max}$ である．すなわち，

$$|\mathfrak{O}_f/\mathfrak{a}\cap\mathfrak{O}_f|=|\mathfrak{O}_{\max}/\mathfrak{a}|$$

であって，ノルムが等しい．特に写像の行き先は $I(\mathfrak{O}_f,f)$ に含まれることがわかった．証明の残りの部分は Lang [60, p.92] にあるので省略する．■

補題 10.9　m を任意の自然数とする．$\mathfrak{O}_f$ の固有イデアルと同値なイデアルで m と素なものが存在する．

証明　原始的な固有イデアルで証明すれば十分である．対応する原始的 2 次形式を，

$$\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$$

として，こちらを同値で取り替えて，a が m と素なことをいえば十分である．m を割り切る素数の集合を S として，

$$S_1=\{p\in S; p\nmid a\},$$

$$S_2=\{p\in S; p|a \text{ かつ } p\nmid c\},$$

$$S_3=\{p\in S; p|a \text{ かつ } p|c\}$$

とする．ここで，$y=\prod_{p\in S_1}p$，$x=\prod_{p\in S_2}p$ とおくと，$(x,y)=1$ であり，$A:=ax^2+bxy+cy^2$ は m と素である．実際 $p\in S_1$ ならば ax^2 は p と素であり $p|y$，また $p\in S_2$ ならば $p|x$ であり，$p\nmid cy^2$ であるから，よって，ともに $p\nmid A$ となる．$p\in S_3$ ならば，もともと a,b,c は互いに素だから，$p\nmid b$ となり，$p\nmid xy$ より，やはり A は p と素である．■

以下，$\mathfrak{O}_{\max}$ のイデアルについて，後で必要な性質を少し復習する．

命題 10.10

(1)　$\mathfrak{O}_{\max}$ の 2 つのイデアル $\mathfrak{a}$，$\mathfrak{b}$ に対し $N(\mathfrak{ab})=N(\mathfrak{a})N(\mathfrak{b})$ である．

(2)　ディリクレ指標 $\chi_K(n)=\left(\frac{D_K}{n}\right)$ について，$\chi_K(N(\mathfrak{a}))=1$ が $\mathfrak{O}_{\max}$ の D_K と素な任意のイデアル $\mathfrak{a}$ について成り立つ．

(3)　逆に (2) の性質を満たす原始的ディリクレ指標で単位指標以外のものは χ_K に限る．

証明　(1) はどの本にも出ているので省略する．(2) は，原始的イデアルについて証明すれば十分である．$\mathfrak{a} = \mathbf{Z}a + \mathbf{Z}(d+\omega)$ として，これが $\mathfrak{O}_{\max}$ のイデアルであるためには $N(d+\omega) = ac$ となる $c \in \mathbf{Z}$ が存在することが条件であった．すなわち，$b = Tr(d+\omega)$ とおいて，$b^2 \equiv D_K \bmod 4a$ が条件である．このためには，もし a と D_K が素ならば，a の各素因子 p について，$\chi_K(p) = 1$ が必要条件である．($p \neq 2$ ならば明らかであるし，$p = 2$ ならば $D_K \equiv 1$ または $5 \bmod 8$ の条件で決まる.)　よって，示された．

(3) の証明は少し面倒なので概要のみを述べる．(2) の性質を満たす単位指標以外の原始的ディィリクレ指標 χ をとる．もし $\chi_K(p) = 1$ ならば $N(\mathfrak{a}) = p$ となるイデアルが存在するのは上の合同式より明らかであり，よって $\chi(p) = 1$ となる．また自然数 a が D_K と素ならば，$\chi(a)^2 = \chi(a^2) = \chi(N(a)) = 1$ であるが，χ が法 m の指標とすると，m と素な任意の自然数 a に対して $a + km$ で D_K と素なものが存在するから，m と素な数 a についてはいつでも $\chi^2(a) = 1$ である．χ は原始的としたから，たとえば p を法とする指標の積に分解することにより，ある 2 次体 K' があって，$\chi = \chi_{K'}$ と書けることがわかる．よって，$K \neq K'$ ならば $\chi_K(p) = -1$ かつ $\chi_{K'}(p) = -1$ となる素数が存在することが，たとえば素数べきの指標に分解し相互法則を用いることなどによりわかるので，$K = K'$ すなわち $\chi = \chi_K$ がわかる．　■

2 次体の極大整環のイデアルの乗法構造について，証明なしで結果を述べておく．(前命題は実はこの構造を使って述べるほうが自然である.)　詳しくは初等整数論の本（たとえば [80]）を参照されたい．

定理 10.11　2 次体 K の極大整環 $\mathfrak{O}_{\max}$ の（0 以外の）イデアルは，素イデアルの積に一意的に表される．また $\mathbf{Z}$ の素数 p は，

（1）　$\chi_K(p) = 1$ ならば，$p\mathfrak{O}_{\max} = \mathfrak{p}_1\mathfrak{p}_2$ と 2 つの素イデアル $\mathfrak{p}_1$，$\mathfrak{p}_2$ の積に分解される．ここで $\mathfrak{p}_2 = \overline{\mathfrak{p}_1}$ となる．ただし

$$\overline{\mathfrak{p}_1} = \{\bar{\alpha};\ \alpha \in \mathfrak{p}_1\}.$$

$x \mapsto \bar{x}$ は $K/\mathbf{Q}$ の自明でない自己同型．

（2）　$\chi_K(p) = -1$ ならば $p\mathfrak{O}_{\max}$ は素イデアルである．

（3）　$\chi_K(p) = 0$ すなわち p が D_K の素因子ならば

$$p\mathfrak{O}_{\max} = \mathfrak{p}^2$$

と，ある素イデアルの 2 乗に分解する．

$\mathfrak{O}_{\max}$ の素イデアルは以上の (1)，(2)，(3) に現れたものに限る．

なお，この定理はゼータ関数の間の関係式を導く．すなわち，2 次体 K に対して，K のデデキント[2]ゼータ関数を

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s}$$

と定義する．ここで和は $\mathfrak{O}_{\max}$ のイデアル全体をわたる．（これは $\mathrm{Re}(s) > 1$ で絶対一様に収束することがわかる.） すると，素イデアル分解の一意性は

$$\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1 - N(\mathfrak{p})^s}$$

というオイラー積を意味する．（ここで積は $\mathfrak{O}_{\max}$ の素イデアル全体をわたる.）

また分解の様子は

$$\zeta_K(s) = \zeta(s)L(s, \chi_K)$$

ということを意味している．あとでこの関係式の直接証明を行う．

10.2 虚 2 次体の類数公式の証明

虚 2 次体の類数がベルヌーイ数で書けるという証明を行う．証明の方法はいろいろ知られているが，ここでは，高木 [80] 等の古典的な教科書では比較的取り上げられていないテータ関数の性質を使う方法を述べる．

定理 10.12 K を虚 2 次体，χ_K を前節最後に述べた K に対応する指標，w を K の極大整環 $\mathfrak{O}_{\max}$ に含まれる 1 のべき根の個数の半分とする．このとき $\mathfrak{O}_K$ の類数は，次式で与えられる．

$$h(D_K) = -wB_{1,\chi_K}.$$

証明のために，テータ関数の変換公式を復習する．a,b,c を整数として，2 次形式 $Q(x,y) = ax^2 + bxy + cy^2$ は正定値と仮定する．また $Q^{-1}(x,y) = 4(4ac - b^2)^{-1}(cx^2 - bxy + ay^2)$ と定義する．$\mathfrak{H} = \{\tau \in \mathbf{C};\ \tau$ の虚部は正 $\}$（上半平面）とおき，$\tau \in \mathfrak{H}$ に対して

---

[2] Julius Wilhelm Richard Dedekind（1831.10.6 ドイツ Braunschweig 生——1916.2.12 ドイツ Braunschweig 没）

$$\theta_Q(\tau) = \sum_{x,y\in\mathbf{Z}} e^{\pi i Q(x,y)\tau}$$

とおく．これは広義絶対一様収束し，τ についての $\mathfrak{H}$ 上の正則関数であることは容易にわかる．

命題 10.13　次の変換法則が成り立つ．

$$\theta_{Q^{-1}}(-\frac{1}{\tau}) = \sqrt{(4ac-b^2)}(\tau/2i)\theta_Q(\tau).$$

証明　証明はたとえば [2, p.25] などに一般論がある．ここでは，この場合に限った直接証明を書いておく．フーリエ[3]変換の理論でよく知られたポアソン[4]の和公式を用いる．記号を簡略にするために，任意の複素数 $z \in \mathbf{C}$ に対して $\mathbf{e}(z) = e^{2\pi i z}$ と書く．$\alpha > 0$ と $\tau \in \mathfrak{H}$ および ξ，$\xi^* \in \mathbf{R}$ に対して

$$\int_{-\infty}^{\infty} \mathbf{e}(2^{-1}\alpha\tau\xi^2)\mathbf{e}(-\xi\xi^*)d\xi = \frac{\mathbf{e}(-(2\tau\alpha)^{-1}\xi^{*2})}{\sqrt{-i\tau\alpha}}$$

となることはよく知られている．ただし，複素数の平方根の分枝は主値，すなわち上の値でいえば $\tau = i$ で $\sqrt{-i\tau\alpha} = \sqrt{\alpha} > 0$ となるものをとっている．

$$f(\xi,\eta) = \mathbf{e}(2^{-1}Q(\xi,\eta)\tau)$$

とすると，この関数の $(\xi,\eta) \in \mathbf{R}^2$ に関するフーリエ変換は次のように計算される．

$$\begin{aligned}
\hat{f}(\xi^*,\eta^*) &= \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(\xi,\eta)\mathbf{e}(-\xi\xi^* - \eta\eta^*)d\xi\,d\eta \\
&= \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \mathbf{e}(2^{-1}\tau(a(\xi + (b/2a)\eta)^2 + (c - b^2/4a)\eta^2)) \\
&\qquad \times \mathbf{e}(-\xi\xi^* - \eta\eta^*)d\xi\,d\eta \\
&= \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \mathbf{e}(2^{-1}\tau(a\xi^2 + (c - b^2/4a)\eta^2)) \\
&\qquad \times \mathbf{e}(-\xi\xi^* - \eta(\eta^* - (b/2a)\xi^*))d\xi\,d\eta
\end{aligned}$$

---

[3]Jean Baptiste Joseph Fourier（1768.3.21 フランス Auxerre 生――1830.5.16 フランス Paris 没）

[4]Siméon Denis Poisson（1781.6.21 フランス Pithiviers 生――1840.4.25 フランス Sceaux 没）

$$= \frac{1}{\sqrt{-i\tau a}\sqrt{-i\tau(c-b^2/4a)}}$$
$$\times \mathbf{e}(-(2\tau a)^{-1}\xi^{*2})\mathbf{e}(-(2\tau(c-b^2/4a))^{-1}(\eta^*-(b/2a)\xi^*)^2)$$
$$= \frac{2i}{\tau\sqrt{(4ac-b^2)}} \times \mathbf{e}\left(\frac{-1}{2\tau(ac-b^2/4)}(a\eta^{*2}-b\eta^*\xi^*+c\xi^{*2})\right).$$

以上のフーリエ変換の公式とポアソンの和公式（たとえば [44, p.227]）によって，

$$\sum_{\xi,\eta\in\mathbf{Z}} f(\xi,\eta) = \sum_{\xi^*,\eta^*\in\mathbf{Z}} \hat{f}(\xi^*,\eta^*)$$

より，テータ関数の変換公式を得る． ∎

類数公式の証明 ゼータ関数の留数の値を 2 通りの方法で計算することにより示す．すなわち，前節の $\zeta_K(s)=\zeta(s)L(s,\chi_K)$ を利用して

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \frac{\pi h(D_K)}{w\sqrt{|D_K|}}$$

および

$$L(1,\chi_K) = \frac{g(\chi)\pi i}{|D_K|}B_{1,\chi_K} = -\frac{B_{1,\chi_K}\pi}{\sqrt{|D_K|}},$$
$$\lim_{s\to 1}(s-1)\zeta(s) = 1$$

から，でるのである．右辺の評価は前章の関数等式その他から容易であるから，ここでのポイントは左辺の評価である．$\mathfrak{O}_{\max}$ のイデアル類を 1 つ固定し，この類に属するイデアル全体の集合を C とする．

$$\zeta(s,C) = \sum_{\mathfrak{a}\in C}\frac{1}{N(\mathfrak{a})^s}$$

とおく． ∎

補題 10.14 C の取り方によらずに

$$\lim_{s\to 1}(s-1)\zeta(s,C) = \frac{\pi}{w\sqrt{|D_K|}}$$

が成立する．

証明 分数イデアル $L \in C$ を 1 つとると，他の C 内のイデアルは $L\alpha$ （$\alpha\in K^\times$）と書けるが，$L\alpha \subset \mathfrak{O}_{\max}$ より，$\alpha \in L^{-1}$ である．$L^{-1}=\mathfrak{a}\subset\mathfrak{O}_{\max}$

となるように L を選んでおける．ここで $\mathfrak{a}$ は原始的イデアルとしても一般性を失わない．また，$L\alpha = L\beta$ であるための必要十分条件は $\alpha = \epsilon\beta$（ϵ は K 内の 1 のべき根）となることである．よって，

$$\zeta(s, C) = \frac{N(\mathfrak{a})^s}{2w} \sum_{\substack{\alpha \in \mathfrak{a} \\ \alpha \neq 0}} \frac{1}{N(\alpha)^s}$$

である．$\mathfrak{a} = \mathbf{Z}a + \mathbf{Z}(d+\omega)$ と標準基底で表し，いつものように $N(d+\omega) = ac$, $b = Tr(d+\omega)$ とおくと $\alpha = xa + y(d+\omega)$ のとき $N(\alpha) = a(ax^2 + bxy + cy^2)$ となる．$N(\mathfrak{a}) = a$ であったから，この部分は分子と打ち消しあう．よって，

$$\zeta(s, C) = \frac{1}{2w} \sum_{x,y \in \mathbf{Z};\ (x,y) \neq (0,0)} (ax^2 + bxy + cy^2)^{-s}$$

である．また $4ac - b^2 = |D_K|$ である．さて，目標はこの関数の $s = 1$ での留数を求めることである．類数公式の証明法の違いは結局ここをどう示すかの違いである．さまざまな方法が知られているが，ここではテータ関数を使う．次のよく知られたガンマ関数の公式

$$\begin{aligned} \frac{\Gamma(s)}{n^s} &= \int_0^\infty e^{-t} \left(\frac{t}{n}\right)^s \frac{dt}{t} \\ &= \int_0^\infty e^{-nt} t^{s-1}\, dt \end{aligned}$$

を用いて，さらに $\mathrm{Re}(s) > 1$ で $\zeta(s, C)$ は絶対一様収束していることにより，和と積分の順序を交換して

$$\begin{aligned} \Gamma(s)\zeta(s, C) &= \frac{1}{2w} \int_0^\infty \sum_{(\xi,\eta) \in \mathbf{Z}^2 - (0,0)} e^{-(a\xi^2 + b\xi\eta + c\eta^2)y} y^{s-1}\, dy \\ &= \frac{\pi^s}{2w} \int_0^\infty (\theta_Q(iy) - 1) y^{s-1}\, dy. \end{aligned}$$

ここで，$\theta_Q(iy) - 1$ は $y \to \infty$ で急減少関数であるから

$$\int_1^\infty (\theta_Q(iy) - 1) y^{s-1}\, dy$$

は任意の $s \in \mathbf{C}$ について収束し，全複素平面で s の正則関数である．

一方，積分範囲を $(0, 1)$ にすると，s が小さいとき，0 の近くで収束しないか

もしれない．こちらを処理するためにテータ関数の変換公式を用いる．すなわち区間 $(0,1)$ の積分で y を y^{-1} に置き換えれば，$\mathrm{Re}(s)>1$ の範囲で，

$$
\begin{aligned}
&\int_0^1 (\theta_Q(iy)-1)y^{s-1}\,dy \\
&= \int_1^\infty (\theta_Q(iy^{-1})-1)y^{-s-1}\,dy \\
&= \int_1^\infty (\theta_{Q^{-1}}(iy)2y\sqrt{|D_K|^{-1}}-1)y^{-s-1}\,dy \\
&= \int_1^\infty \{2(\theta_{Q^{-1}}(iy)-1)y^{-s}\sqrt{|D_K|^{-1}}+2y^{-s}\sqrt{|D_K|^{-1}}-y^{-s-1}\}dy \\
&= 2\int_1^\infty (\theta_{Q^{-1}}(iy)-1)\frac{y^{-s}}{\sqrt{|D_K|}}\,dy-\frac{2}{\sqrt{|D_K|}(1-s)}-\frac{1}{s}.
\end{aligned}
$$

最後の式の積分は任意の s で収束するので全複素平面で正則であり，残りの部分は極である．よって，$\zeta(s,C)$ の $s=1$ での留数は

$$
\frac{1}{\Gamma(1)}\frac{1}{2w}\times\frac{2\pi}{\sqrt{|D_K|}}=\frac{\pi}{w\sqrt{|D_K|}}.
$$

よって，補題は示された．ゆえに

$$
\lim_{s\to 1}(s-1)\zeta_K(s)=\frac{h\pi}{w\sqrt{|D_K|}}
$$

となるのである．これと，$L(1,\chi_K)$ の値を比較して類数公式を得る． ∎

さて，$\zeta(s)$ と $L(s,\chi)$ は関数等式をもっていたから，その積である $\zeta_K(s)$ も関数等式をもつし，具体的な形を計算することも容易である．ところで，いまの積分表示を使えば，実は $\zeta(s,C)$ の解析接続と関数等式が得られ，これから $\zeta_K(s)$ の解析接続と関数等式の別証が得られる．すなわち

命題 10.15 C を虚 2 次体 K の極大整環 $\mathfrak{O}_{\max}$ のイデアル類とし，その他の記号を上のとおりとする．$\zeta(s,C)$ は全 s 平面に有理型に解析接続され，$\xi(s,C)=(2\pi)^{-s}|D_K|^{s/2}\Gamma(s)\zeta(s,C)$ とおくと，関数等式

$$
\xi(1-s,C)=\xi(s,C)
$$

を満たす．同様に，$\xi_K(s)=(2\pi)^{-s}|D_K|^{s/2}\Gamma(s)\zeta_K(s)$ とおくと，

$$
\xi_K(1-s)=\xi_K(s)
$$

がわかる．

証明 解析接続と関数等式の証明は前に述べた積分表示を用いる．$\mathrm{Re}(s)>1$

において

$$
\begin{aligned}
&(2w)\pi^{-s}\Gamma(s)\zeta(s,C)\\
&\quad=\int_1^\infty (\theta_Q(iy)-1)y^{s-1}\,dy\\
&\qquad+\frac{2}{\sqrt{|D_K|}}\int_1^\infty (\theta_{Q^{-1}}(iy)-1)y^{-s}\,dy-\frac{2}{\sqrt{|D_K|}(1-s)}-\frac{1}{s}
\end{aligned}
$$

であるが，右辺の積分の部分は全 s 平面で正則であるから，右辺は全複素 s 平面で有理型な関数になっている．よって解析接続は証明された．

関数等式は，前の積分表示の両辺に $2^{-s}|D_K|^{s/2}$ をかけた後に $s\to 1-s$ とすると，

$$
\begin{aligned}
(2w)\xi(1-s,C)&=(2w)|D_K|^{(1-s)/2}(2\pi)^{s-1}\Gamma(1-s)\zeta(1-s,C)\\
&=2^{s-1}|D_K|^{(1-s)/2}\int_1^\infty (\theta_Q(iy)-1)y^{-s}\,dy\\
&\quad+2^s|D_K|^{-1/2}|D_K|^{(1-s)/2}\int_1^\infty (\theta_{Q^{-1}}(iy)-1)y^{s-1}\,dy\\
&\quad-\frac{2^s|D_K|^{(1-s)/2}|D_K|^{-1/2}}{s}-\frac{2^{s-1}|D_K|^{(1-s)/2}}{1-s}\\
&=2^s|D_K|^{-s/2}\left(2^{-1}|D_K|^{1/2}\int_1^\infty (\theta_Q(iy)-1)y^{-s}\,dy\right.\\
&\quad\left.+\int_1^\infty (\theta_{Q^{-1}}(iy)-1)y^{s-1}\,dy-\frac{1}{s}-\frac{2^{-1}|D_K|^{1/2}}{1-s}\right).
\end{aligned}
$$

ここで，

$$
4\begin{vmatrix} a & b/2\\ b/2 & c\end{vmatrix}^{-1}=16|D_K|^{-1}
$$

に注意すると，

$$
\begin{aligned}
&\int_0^\infty (\theta_{Q^{-1}}(iy)-1)y^{s-1}dy\\
&\quad=\int_1^\infty (\theta_{Q^{-1}}(iy)-1)y^{s-1}dy\\
&\qquad+2^{-1}\sqrt{|D_K|}\int_1^\infty (\theta_Q(iy)-1)y^{-s}dy-\frac{2^{-1}\sqrt{|D_K|}}{1-s}-\frac{1}{s}
\end{aligned}
$$

となることがわかる．よって

$$(2w)\xi(1-s,C) = 2^s|D_K|^{-s/2}\int_0^\infty (\theta_{Q^{-1}}(iy)-1)y^{s-1}\,dy$$

である．この右辺を解釈するために，Q^{-1} を調べる．まず

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} c & -b/2 \\ -b/2 & a \end{pmatrix}$$

によって，$cx^2-bxy+ay^2$ は $ax^2+bxy+cy^2$ と同値である．したがって，$\zeta(s,C)$ は $\theta_{Q^{-1}}(\tau)$ を用いて表すこともできる．すなわち

$$Q^{-1}(x,y)^{-s} = 2^{-2s}|D_K|^s(cx^2-bxy+ay^2)^{-s}$$

であるから，前と同様にして

$$(2w)\Gamma(s)\zeta(s,C) = 2^{2s}\pi^s|D_K|^{-s}\int_0^\infty (\theta_{Q^{-1}}(iy)-1)y^{s-1}\,dy$$

がわかる．これより，前の計算と合わせて，

$$\begin{aligned}(2w)\xi(1-s,C) &= (2\pi)^{-s}|D_K|^{s/2}2^{2s}|D_K|^{-s}\pi^s\int_0^\infty (\theta_{Q^{-1}}(iy)-1)y^{s-1}\,dy \\ &= (2w)(2\pi)^{-s}|D_K|^{s/2}\Gamma(s)\zeta(s,C) = (2w)\xi(s,C).\end{aligned}$$

よって，命題は証明された．$\xi_K(s)$ の関数等式はこれより明らかである． ∎

任意の整環の場合には，$\mathfrak{O}_f$ のイデアル類群の類数 $h(f^2D_K)$ の公式は，$\mathfrak{O}_{\max}$ のイデアル類群との群論的な比較で求めるのが最も容易である（たとえば，Weber [89, p.366]，Lang [60, p.95]，Zagier [93] などを参照.） しかしここではあえて異なる方法を紹介しよう．

いままでは K が虚 2 次体の場合を扱ったが，これからしばらく K は虚または実の 2 次体とする．自然数 f を固定して，K の整環 $\mathfrak{O}_f = \mathbf{Z}+\mathbf{Z}f\omega$ のイデアルについてのゼータ関数を考える．すなわち

$$\zeta(s,f^2D_K) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s}.$$

ここで和は $\mathfrak{O}_f$ の（固有イデアルとは限らない）任意のイデアルを動くとする．

命題 10.16

(1) 正の整数 a に対して $r(a)$ を $b^2 \equiv f^2D_K \bmod 4a$ なる整数 b を $\bmod 2a$ で数えた個数とすると，

$$\zeta(s, f^2 D_K) = \zeta(2s) \sum_{a=1}^{\infty} r(a) a^{-s}$$

である．

（2）さらに詳しく次が成り立つ．

$$\zeta(s, f^2 D_K) = \zeta(s) L(s, \chi_K) \prod_{\substack{p \mid f \\ p^m \parallel f}} \frac{1 - p^{(m+1)(1-2s)} - \chi_K(p) p^{-s} (1 - p^{m(1-2s)})}{1 - p^{1-2s}}.$$

ここに m は f を割る p の最高べきである（したがって p による）．

証明　$\mathfrak{O}_f$ の原始的イデアルは $\mathfrak{a} = \mathbf{Z}a + \mathbf{Z}(d + f\omega)$（$a = N(\mathfrak{a})$）と書け，さらに $N(d + f\omega) = ac$ となる整数 c が存在する．すなわち $b = 2d + fTr(\omega)$ とおいて，$b^2 \equiv f^2 D_K \bmod 4a$ となるのであった（79 ページ補題 6.2 と 80 ページ補題 6.4）．$\mathbf{Z}a + \mathbf{Z}(d + f\omega) = \mathbf{Z}a' + \mathbf{Z}(d' + f\omega)$（$a, a' > 0$）ならば，$a = a'$ かつ $d \equiv d' \bmod a$ となる．よって，a を固定するとき，$b = 2d + fTr(\omega)$ と $b' = 2d' + fTr(\omega)$ について $b \equiv b' \bmod 2a$ がイデアルが等しいための条件である．原始的でないものまで考慮に入れて，(1) が証明された．

次に (2) を示す．これには $r(a)$ を計算すればよい．中国の剰余定理により，各素数のべきについて求めておけばよい．$a = p^e$ とする．まず，p を奇数とする．$f = p^m f_0$, f_0 は p と素としよう．$b^2 \equiv p^{2m} D_K \bmod p^e$ と考えて，$e \leq 2m$ ならば $b^2 \equiv 0 \bmod p^e$．よって，$e = 2e_0$ ならば $b \equiv 0 \bmod p^{e_0}$，$e = 2e_0 - 1$ ならば $b \equiv 0 \bmod p^{e_0}$．よって，$\bmod p^e$ では，b は p^{e_0} または $p^{e_0 - 1}$ 個ある．つまり $r(p^{2e_0}) = p^{e_0}$，$r(p^{2e_0 - 1}) = p^{e_0 - 1}$．また，$2m < e$ ならば，$b = p^m b_0$，$b_0^2 \equiv D_K \bmod p^{e-2m}$ である．まず $p | D_K$ ならば，D_K は p でちょうど 1 回だけ割れるから $e - 2m \geq 2$ なら解はない．よって $e - 2m = 1$ のときだけ解があり，このとき $p | b_0$ すなわち $p^{m+1} | b$ が条件となり $r(p^{2m+1}) = p^m$，$r(p^e) = 0$ $(e > 2m+1)$ である．もし $p \nmid D_K$ ならば，$b_0^2 \equiv D_K \bmod p^{e-2m}$ は $\chi_K(p) = 1$ のときのみ解が $\bmod p^{e-2m}$ で 2 つあり，これを $\bmod p^{e-m}$ で数えるので $2p^m$ 個．結局 $p \nmid D_K$，$e > 2m$ ならば，e によらずに $r(p^e) = p^m(1 + \chi_K(p))$ となる．これらから

$$\sum_{e=0}^{\infty} r(p^e)p^{-es} = \frac{(1+p^{-s})-(1+p^{s-1})p^{(1-2s)(m+1)}}{1-p^{1-2s}}$$
$$+\begin{cases} p^{m(1-2s)-s} & p|D_K \text{ の場合}, \\ \dfrac{(1+\chi_K(p))p^{m(1-2s)-s}}{1-p^{-s}} & p\nmid D_K \text{ の場合} \end{cases}$$

と計算される．最後の場合分けの項は $\dfrac{(1+\chi_K(p))p^{m(1-2s)-s}}{1-\chi_K(p)p^{-s}}$ と書けば統一的に表されることに注意して，通分して計算すると右辺は

$$\frac{(1+p^{-s})(1-p^{(m+1)(1-2s)}-\chi_K(p)p^{-s}(1-p^{m(1-2s)}))}{(1-\chi_K(p)p^{-s})(1-p^{1-2s})}$$

となる．したがってこれに $\zeta(2s)$ のオイラー p 因子をかけて

$$(1-p^{-2s})^{-1}\sum_{e=0}^{\infty} r(p^e)p^{-es} = \frac{1-p^{(m+1)(1-2s)}-\chi_K(p)p^{-s}(1-p^{m(1-2s)})}{(1-p^{-s})(1-\chi_K(p)p^{-s})(1-p^{1-2s})}$$

となる．$p=2$ の場合は，$b^2 = p^{2m}f_0^2D_K \bmod p^{2+e}$ の解を $\bmod p^{1+e}$ で数えることと，$D_K \equiv 0 \bmod 8$，$D_K \equiv 4 \bmod 8$ のことがある点が前と多少異なっている．しかし，もし $D_K \equiv 4 \bmod 8$ ならば $D_K/4 \equiv 3 \bmod 4$ であることなどを用いると，前と類似の計算ができて，

$$r(2^e) = \begin{cases} 2^{[e/2]} & 0 \le e \le 2m, \\ (1+\chi_K(2))2^m & 2m+1 \le e \text{ かつ } D_K \text{ が奇数}, \\ 2^m & e = 2m+1 \text{ かつ } D_K \text{ が偶数}, \\ 0 & 2m+2 < e \text{ かつ } D_K \text{ が偶数}. \end{cases}$$

これを用いて前と同様にゼータ関数の p 因子の部分を計算すると，結果の形は p が奇数のときとまったく同様になり命題は証明された．■

次に，

$$\zeta(s, \mathfrak{O}_f) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s}$$

とおく．ただし今度は，和は $\mathfrak{O}_f$ の固有イデアルのみをとる．

ここでメービウス[5]の関数 $\mu(m)$ を導入する．これは自然数上の，$\{0, \pm 1\}$ に

[5] August Ferdinand Möbius（1790.11.17 ドイツ Schulpforta 生——1868.9.26 ドイツ Leipzig 没）

値をとる関数で次のように定義される．

（1）　$\mu(1)=1$,

（2）　$m = p_1 \cdots p_r$ と異なる r 個の素数の積に素因数分解されるときは $\mu(m)=(-1)^r$,

（3）　m が平方因子をもつとき，すなわちある素数の 2 乗で割り切れるときは $\mu(m)=0$.

m_1 と m_2 が互いに素な自然数ならば $\mu(m_1)\mu(m_2)=\mu(m_1m_2)$ である．

次の公式はメービウスの反転公式として知られている．

補題 10.17　$F(n)$, $G(n)$ をすべての自然数 n について定義された関数とする．ここで任意の自然数 n に対して

$$F(n)=\sum_{d|n} G(d)$$

が成り立つと仮定すると，任意の自然数 n に対して

$$G(n)=\sum_{d|n}\mu(\frac{n}{d})F(d)$$

が成り立つ．

証明は容易であるから省略する．

命題 10.18

（1）　μ をメービウスの関数として

$$\zeta(s,f^2D_K)=f^{-s}\sum_{e|f}e^s\zeta(s,\mathfrak{O}_e),$$

$$\zeta(s,\mathfrak{O}_f)=f^{-s}\sum_{d|f}\mu(f/d)d^s\zeta(s,d^2D_K).$$

である．

（2）　次が成り立つ．

$$\zeta(s,\mathfrak{O}_f)=\zeta(s)L(s,\chi_K)$$
$$\times\prod_{\substack{p|f\\ p^m\|f}}\frac{(1-p^{-s})(1-\chi_K(p)p^{-s})-p^{m-1-2sm}(1-p^{1-s})(\chi_K(p)-p^{1-s})}{1-p^{1-2s}}$$

証明　(1) の第 1 式は，$\mathfrak{O}_f$ のイデアルはある $\mathfrak{O}_e(e|f)$ の固有イデアルである

こと，$\mathfrak{O}_e$ のイデアルと見たときのノルムは f/e 倍されることによる．第 2 式は第 1 式からメービウスの反転公式によりでる．(2) は (1) の第 2 式の右辺を命題 10.16 を用いて計算する．このとき，メービウス関数の性質から，$f = \prod p_i^{m_i}$ のとき d としては $\prod p_i^{m_i - j_i}$，$j_i = 0, 1$ の形のものだけを走らせればよいことに注意すると，命題 10.16 の（$\zeta(s)L(s,\chi_K)$ に含まれない）オイラー因子から，それの m を $m-1$ にかえたものの p^{-s} 倍を引いたものが求めるオイラー因子になることがわかり，結果を得る． ∎

注意 10.19　命題 10.16, 10.18 のゼータ関数の具体的表示は [93], [48] で与えられた．その応用についてはそれぞれの論文を参照されたい．

さて，K が虚 2 次体のときに，以上の $\zeta(s, \mathfrak{O}_f)$ の公式により $\mathfrak{O}_f$ の類数を求める．前と同様，C を $\mathfrak{O}_f$ の固有イデアルのイデアル類として，

$$\zeta(s, C, \mathfrak{O}_f) = \sum_{\mathfrak{a} \in C} \frac{1}{N(\mathfrak{a})^s}$$

とおく．w_f を $\mathfrak{O}_f$ 内の 1 のべき根の個数の半分とする．判別式が $f^2 D_K$ の C と対応する原始的 2 次形式 $Q(x,y) = ax^2 + bxy + cy^2$ について，

$$(2w_f)\zeta(s, C, \mathfrak{O}_f) = \sum_{(x,y) \in \mathbf{Z}^2 - (0,0)} (ax^2 + bxy + cy^2)^{-s}$$

となるのは極大整環のときと同様である．$\theta_Q(\tau)$ の変換公式を用いれば，このディリクレ級数の $s = 1$ での留数は前とまったく同様の方法で計算できて，C によらずに

$$\lim_{s \to 1} (s-1)\zeta(s, C, \mathfrak{O}_f) = \frac{\pi}{w_f f \sqrt{|D_K|}}$$

となる．これより，

$$\lim_{s \to 1} (s-1)\zeta(s, \mathfrak{O}_f) = h(f^2 D_K) \frac{\pi}{w_f f \sqrt{|D_K|}}$$

である．一方，$\zeta(s, \mathfrak{O}_f)$ の命題 10.18 の公式のオイラー積表示をそのまま用いて

$$\lim_{s\to 1}(s-1)\zeta(s,\mathfrak{O}_f)=\left(\lim_{s\to 1}(s-1)\zeta_K(s)\right)\times\prod_{p|f}(1-\chi_K(p)p^{-1})$$
$$=\frac{\pi h(D_K)}{w\sqrt{|D_K|}}\prod_{p|f}(1-\chi_K(p)p^{-1}).$$

よって，類数公式

$$h(f^2D_K)=\frac{h(D_K)}{w/w_f}\times f\prod_{p|f}(1-\chi_K(p)p^{-1})$$

を得る．

実 2 次体 K（ないしは不定符号 2 次形式）の類数公式はこれに比べるとかなり面倒であり，またベルヌーイ数という立場から離れるので省略する．

10.3　L 関数

この節の内容については [40] に基づく．

p を素数とし，$p\equiv 3 \bmod 4$ と仮定する．法 p のディリクレ指標 ψ を，$\psi(a)=\left(\frac{a}{p}\right)$ で定義する．これから任意の 2 次半整数対称行列（その全体を L^* と書いた）上の関数 $\widetilde{\psi}$ を次のように定義する．まず

$$T=\begin{pmatrix}a & b/2\\ b/2 & c\end{pmatrix}\in L^*$$

について，$T\equiv 0 \bmod p$ または $\det(T)\not\equiv 0 \bmod p$ ならば $\widetilde{\psi}(T)=0$ とおく．また

$$T\not\equiv 0 \bmod p \qquad \text{かつ} \qquad \det(T)\equiv 0 \bmod p$$

となる場合は，$g\in GL_2(\mathbf{Z}/p\mathbf{Z})$ で，

$${}^t gT\,g\equiv\begin{pmatrix}e & 0\\ 0 & 0\end{pmatrix} \bmod p$$

となるものが存在する．実際 $T \bmod p$ の階数が 1 だから $Tg \bmod p$ の第 2 列が 0 であるような g が存在し，よって ${}^t gTg$ の第 2 列も 0 であるが，これが対称行列であることより，$(2,1)$ 成分も 0 である．さらに $\psi(e)$ の値は T のみにより，g

の取り方にはよらないことも容易にわかる．これを用いて $\widetilde{\psi}(T)=\psi(e)$ とおく．

2 次正定値半整数対称行列の全体を L_+^* と書くことにする．T_1，$T_2\in L^*$ は，ある $g\in SL_2(\mathbf{Z})$ について ${}^t gT_1g=T_2$ のときに同値というのであった（76 ページ）．L_+^* の指標 $\widetilde{\psi}$ つきの L 関数を

$$L(s,L_+^*,\psi)=\sum_{T\in L_+^*/\sim}\frac{\widetilde{\psi}(T)}{\epsilon(T)\det(T)^s}$$

と定義する．ここで，$L_+^*/\sim$ は L_+^* 内の同値類の完全代表系を意味し，$\epsilon(T)$ は有限群 $\{g\in SL_2(\mathbf{Z});\ {}^t gTg=T\}$ の位数である．（この L 関数がはじめて定義されたのは保型形式の次元公式との関連で，橋本喜一朗氏による．）

少し例を計算してみることにしよう．$p=3$ の場合，

$$\widetilde{\psi}\begin{pmatrix}1 & 1/2\\ 1/2 & 1\end{pmatrix}=1,\quad \widetilde{\psi}\begin{pmatrix}1 & 0\\ 0 & 3\end{pmatrix}=1,\quad \widetilde{\psi}\begin{pmatrix}2 & 1\\ 1 & 2\end{pmatrix}=-1,$$
$$\widetilde{\psi}\begin{pmatrix}1 & 1/2\\ 1/2 & 7\end{pmatrix}=1,\quad \widetilde{\psi}\begin{pmatrix}3 & 3/2\\ 3/2 & 3\end{pmatrix}=0,\cdots$$

これから

$$L(s,L_+^*,\psi)=\frac{2^{2s}}{6\cdot 3^s}+\frac{1}{3\cdot 3^s}+\frac{2^{2s}}{2\cdot 3^{3s}}+\cdots=\frac{2^{2s-1}}{3^{s+1}}+\frac{1}{3^{s+1}}+\frac{2^{2s-1}}{3^{3s}}+\cdots$$

などとなる．

定理 10.20　この L 関数は実は本質的にはリーマンゼータ関数である．すなわち

$$L(s,L_+^*,\psi)=-\frac{2^{2s-1}B_{1,\psi}}{p^s}\zeta(2s-1).$$

特に任意の自然数 m について

$$L(1-m,L_+^*,\psi)=\frac{p^{m-1}}{2^{2m}\cdot m}B_{2m}B_{1,\psi}$$

である．

これを証明する前に補題を 1 つ示しておく．虚 2 次体 K とその判別式 D_K，および正整数 f について $d=f^2D_K$ とおき，

$$\mathcal{P}(d) = \{T = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \in L_+^{*,\mathrm{prim}};\ 4ac - b^2 = -d\}$$

とおく．$L_+^{*,\mathrm{prim}}$ は L_+^* の中で原始的なものの全体である．また $\mathcal{S}(d) = \mathcal{P}(d)/\sim$ とおく．

補題 10.21　d は p で割り切れるとする．

（1）　$\mathbf{Q}(\sqrt{d}) \neq \mathbf{Q}(\sqrt{-p})$ ならば $\displaystyle\sum_{T \in \mathcal{S}(d)} \widetilde{\psi}(T) = 0$ である．

（2）　$\mathbf{Q}(\sqrt{d}) = \mathbf{Q}(\sqrt{-p})$ ならば任意の $T \in \mathcal{P}(d)$ について $\widetilde{\psi}(T) = 1$ である．

証明　$\widetilde{\psi}(T)$ は T に対応するイデアルのノルムでの ψ の値であることをまず見よう．定義により，ある互いに素な整数 x，y が存在して $\widetilde{\psi}(T) = \psi(e)$，$e = ax^2 + bxy + cy^2$ となっている．$4ae = (2ax + by)^2 + (4ac - b^2)y^2$ であり，$4ac - b^2$ は p で割り切れるから，$\psi(ae) = \psi(2ax + by)^2$ である．仮定により $p \nmid e$ であり，また必要なら同値なものに取り替えて $p \nmid a$ と仮定してもよい．よって，$\psi(2ax + by) \neq 0$ であり，$\psi(2ax + by)^2 = 1$，ゆえに $\psi(a) = \psi(e)$ である．ゆえにこれはノルムの値である．よって $K = \mathbf{Q}(\sqrt{d}) = \mathbf{Q}(\sqrt{-p})$ ならば，$\chi_K = \psi$ であるから，命題 10.10 により，$\widetilde{\psi}(T) = 1$ となる．もし $K = \mathbf{Q}(\sqrt{d}) \neq \mathbf{Q}(\sqrt{-p})$ ならば，$\chi_K \neq \psi$ であるから，$\widetilde{\psi}(T)$ は $\mathcal{S}(d)$ のある元で -1 となる．すなわち $\widetilde{\psi}$ は群 $\mathcal{S}(d)$ 上の，単位指標以外の指標であるから，群上での和は 0 になる．∎

定理 10.20 の証明　まず p と素な整数 e と $T \in L_+^*$ について，$\widetilde{\psi}(eT) = \psi(e)\widetilde{\psi}(T)$ は明らかであり，また $\epsilon(eT) = \epsilon(T)$ であるから，L 関数を原始的 2 次形式の和に帰着できる．すなわち

$$L^{\mathrm{prim}}(s, L_+^*, \psi) = \sum_{T \in L^{*,\mathrm{prim}}/\sim} \frac{\widetilde{\psi}(T)}{\epsilon(T) \det(T)^s}$$

とおくと

$$\begin{aligned}
L(s, L_+^*, \psi) &= \sum_{e=1}^{\infty} \sum_{T \in L_+^{*,\mathrm{prim}}/\sim} \frac{\psi(e)\widetilde{\psi}(T)}{\epsilon(eT)\det(eT)^s} \\
&= \sum_{e=1}^{\infty} \frac{\psi(e)}{e^{2s}} L^{\mathrm{prim}}(s, L_+^*, \psi) \\
&= L(2s, \psi) L^{\mathrm{prim}}(s, L_+^*, \psi).
\end{aligned}$$

ここで $L(2s,\psi)$ はディリクレの L 関数である．次に $L_+^{*,\mathrm{prim}}$ について，前の補題を用いると，$4\det(T) = -d = f^2 p$（f は正整数）の部分だけ生き残る．$\epsilon(T)$ は $\mathcal{P}(d)$ について共通であるから，これを $\epsilon(d)$ と書くと，

$$L^{\mathrm{prim}}(s, L_+^*, \psi) = 2^{2s} \sum_{f=1}^{\infty} \frac{|\mathcal{S}(d)|}{p^s f^{2s} \epsilon(d)}$$

となる．原始的 2 次形式と 2 次体の整環の原始的な固有イデアルとの関係により，$|\mathcal{S}(d)|$ は，虚 2 次体 $K = \mathbf{Q}(\sqrt{-p})$ の整環 $\mathcal{O}_f$ の類数 $h(f^2 D_K)$ である．類数公式によって

$$L^{\mathrm{prim}}(s, L_+^*, \psi) = 2^{2s} \frac{h(D_K)}{|\mathcal{O}_{\max}| p^s} \sum_{f=1}^{\infty} f^{1-2s} \prod_{\substack{q|f \\ q:\mathrm{prime}}} (1 - \frac{1}{q}\psi(q)).$$

ここで

$$\frac{h(D_K)}{|\mathcal{O}_{\max}| p^s} = -\frac{B_{1,\psi}}{2p^s}$$

であった．

$$\begin{aligned}
\sum_{f=1}^{\infty} f^{1-2s} \prod_{q|f} (1 - \frac{1}{q}\psi(q)) &= \sum_{f=1}^{\infty} f^{1-2s} \prod_{\substack{q|f \\ q:\mathrm{prime}}} (1 + \frac{1}{q}\psi(q)\mu(q)) \\
&= \sum_{f=1}^{\infty} f^{1-2s} \sum_{m|f} \frac{1}{m}\psi(m)\mu(m).
\end{aligned}$$

ここで $f = mn$ と置き換えれば，上の和は

$$\begin{aligned}
\sum_{m,n=1}^{\infty} n^{1-2s} m^{-2s} \psi(m)\mu(m) &= \zeta(2s-1) \prod_{q:prime} (1 - \psi(q) q^{-2s}) \\
&= \zeta(2s-1) L(2s, \psi)^{-1}
\end{aligned}$$

となる．以上を合わせて定理の $L(s, L_+^*, \psi)$ の表示を得る．特殊値については，

リーマンゼータ関数の 0 以下の整数での値が $\zeta(1-m) = -B_m/m$（72 ページ定理 5.4）であったから，直ちにでる. ∎

以上の比較的やさしい考察は，対称行列のなす概均質ベクトル空間のゼータ関数が実はやさしい対象なのではないかと考え始めるきっかけとなった. 結果的には任意のサイズの対称行列について，やさしい対象であることがわかり，保型形式の次元公式などに決定的な応用をもつにいたった. これらの発展については [39], [41], [42] などを参照されたい.

第 11 章

p 進測度とクンマー合同式

現代の数論において，p 進的な考え方が 1 つの重要な役割を果たしている．たとえば，ディリクレ L 関数に対応して p 進 L 関数というものがある．実は 3.3 節で述べたクンマー合同式は，正しく補正（オイラー因子による）を行うと，この p 進 L 関数の存在を保証している合同式であると解釈される．したがってこの合同式は，p 進 L 関数の文脈で理解し，証明を与えるのが最も自然な方法であるといえよう．しかしながら，本格的に p 進 L 関数を論ずるのは本書の枠外であるので，その導入として以下において，ベルヌーイ数をある p 進積分で表し，それを用いてクンマー合同式を証明しよう．さらに進んで本格的に勉強しようという方は，岩澤 [45], Washington [88], Lang [59] 等の教科書を参照されたい．

この章では p 進数の知識を仮定する．これについてはたとえば Serre [73, 第 1 章] 参照．この章の結果を他の章で使うことはない．

11.1 p 進整数環上の測度と形式的べき級数環

次節で p 進整数環上にベルヌーイ測度と呼ばれる測度を定義し，ベルヌーイ数を積分の形に表示する．このような表示がクンマー合同式を証明するのに大変役に立つ．

ここではそのための準備として p 進整数環 $\mathbf{Z}_p$ 上の測度と形式的べき級数環との対応の一般論を解説する．

$\overline{\mathbf{Q}}_p$ を p 進数体 $\mathbf{Q}_p$ の代数的閉包とすると，$\mathbf{Q}_p$ の p 進絶対値 $|\ |$（$|p|=1/p$ と正規化する）は $\overline{\mathbf{Q}}_p$ の p 進絶対値に一意的に伸びる．それも $|\ |$ で表す．このとき，$\overline{\mathbf{Q}}_p$ は完備にはならないので，$\overline{\mathbf{Q}}_p$ の $|\ |$ に関する完備化を $\mathbf{C}_p$ と記す．$|\ |$ は $\mathbf{C}_p$ 上に自然に伸びる．$\mathcal{O}_p$ を $\mathbf{C}_p$ の整数環とする．すなわち

$$\mathcal{O}_p = \{x \in \mathbf{C}_p \mid |x| \leq 1\}.$$

注意 11.1　なぜこういう大きな体を用意するのかは，$\mathbf{Q}_p$ 上の解析をするための容器が必要なためである．有理数体 $\mathbf{Q}$ の代数的閉包 $\overline{\mathbf{Q}}$ は通常の位相に関して完備ではなく，複素数体 $\mathbf{C}$ の中で考えるのと似た状況である．

最初に $\mathbf{Z}_p$ 上の測度の一般論を述べる．

$\mathbf{Z}$ 加群 $\mathbf{Z}/p^n\mathbf{Z}$ を X_n と記し，X_{n+1} から X_n への標準的全射 π_{n+1} を

$$\pi_{n+1} : X_{n+1} \ni x \bmod p^{n+1}\mathbf{Z} \longmapsto x \bmod p^n\mathbf{Z} \in X_n$$

とする．X_n と π_n の組 (X_n, π_n) から射影極限 $\varprojlim X_n$ が

$$\varprojlim X_n = \left\{(x_n) \in \prod_{n\geq 1} X_n \mid \pi_{n+1}(x_{n+1}) = x_n\right\}$$

で定義される．このとき，p 進整数環 $\mathbf{Z}_p$ は射影極限 $\varprojlim X_n$ と同一視される．

定義 11.2（**$\mathbf{Z}_p$ 上の測度**）　$\mu = \{\mu_n\}_{n=1}^{\infty}$ が $\mathbf{Z}_p$ 上の $\mathcal{O}_p$ 値測度であるとは，

(i)　$\mu_n : X_n \longrightarrow \mathcal{O}_p$ で，かつ

(ii)　任意の $n \in \mathbf{N}$，$x \in X_n$ に対して，性質（distribution property）

$$\mu_n(x) = \sum_{y \in X_{n+1},\ \pi_{n+1}(y)=x} \mu_{n+1}(y)$$

を満たすときをいう．

$\mathbf{Z}_p$ 上の $\mathcal{O}_p$ 値測度の全体を $\mathcal{M}(\mathbf{Z}_p, \mathcal{O}_p)$ と記す．$\mathcal{M}(\mathbf{Z}_p, \mathcal{O}_p)$ には $\mathcal{O}_p$ 加群の構造が入る．$\mu = \{\mu_n\} \in \mathcal{M}(\mathbf{Z}_p, \mathcal{O}_p)$ のノルムは

$$\|\mu\| = \max_{n\in\mathbf{N},\ x\in X_n} |\mu_n(x)|$$

で定義される．

また $\mathbf{Z}_p$ 上の $\mathcal{O}_p$ 値連続関数のなす $\mathcal{O}_p$ 加群を $C(\mathbf{Z}_p, \mathcal{O}_p)$と記す．$\varphi \in C(\mathbf{Z}_p, \mathcal{O}_p)$ のノルム $\|\varphi\|$ が

$$\|\varphi\| = \max_{x \in \mathbf{Z}_p} |\varphi(x)|$$

で定義される．いま，$\varphi \in C(\mathbf{Z}_p, \mathcal{O}_p)$ と $\mu = \{\mu_n\} \in \mathcal{M}(\mathbf{Z}_p, \mathcal{O}_p)$ に対して $\mathbf{Z}_p$ 上の積分を次のように定義する．

$$\int_{\mathbf{Z}_p} \varphi(x) d\mu(x) = \lim_{n \to \infty} \sum_{r=0}^{p^n-1} \varphi(r) \mu_n(r).$$

（$\mu_n(r \bmod p^n)$ を $\mu_n(r)$ と略記している．以下においても同様.）ここで右辺の極限が収束するのは，次の評価による．$n < m$ のとき，

$$\left| \sum_{r=0}^{p^n-1} \varphi(r)\mu_n(r) - \sum_{l=0}^{p^m-1} \varphi(l)\mu_m(l) \right|$$

$$= \left| \sum_{r=0}^{p^n-1} \Big(\varphi(r)\mu_n(r) - \sum_{q=0}^{p^{m-n}-1} \varphi(r+p^n q)\mu_m(r+p^n q) \Big) \right|$$

$$= \left| \sum_{r=0}^{p^n-1} \sum_{q=0}^{p^{m-n}-1} \big(\varphi(r) - \varphi(r+p^n q)\big) \mu_m(r+p^n q) \right|$$

$$\leq \max_{r,\, q} \big|\varphi(r) - \varphi(r+p^n q)\big| \, \|\mu\|.$$

各自然数 k に対し，X の 2 項多項式を

$$\binom{X}{k} = \frac{X(X-1)\cdots(X-k+1)}{k!}$$

で定義すると，$\mathbf{Z}_p$ 上の連続関数になる．

$\mu = \{\mu_n\} \in \mathcal{M}(\mathbf{Z}_p, \mathcal{O}_p)$ に対し，次のように $f \in \mathcal{O}_p[[X]]$ を対応させる．$\Lambda = \mathcal{O}_p[[X]]$, $\Lambda_n = ((1+X)^{p^n} - 1)\Lambda$ とおき，自然な写像 $\varpi_n : \Lambda/\Lambda_n \longrightarrow \Lambda/\Lambda_{n-1}$ によって射影系 $\{(\Lambda/\Lambda_n, \varpi_n)\}$ を考える．いま，$f_n(X) \in \Lambda/\Lambda_n$ を

$$f_n(X) = \sum_{r=0}^{p^n-1} \mu_n(r)(1+X)^r = \sum_{r=0}^{p^n-1} \sum_{k=0}^{r} \mu_n(r) \binom{r}{k} X^k$$

$$= \sum_{k=0}^{p^n-1} c_{n,k} X^k$$

とする（$\bmod \Lambda_n$ で考える）．ただし

$$c_{n,k} = \sum_{r=0}^{p^n-1} \mu_n(r)\binom{r}{k}$$

とおいた．

$$(\varpi_n f_n)(X) = \varpi_n\left(\sum_{r=0}^{p^n-1} \mu_n(r)(1+X)^r\right)$$

$$= \varpi_n\left(\sum_{r'=0}^{p^{n-1}-1}\sum_{l=0}^{p-1} \mu_n(r'+p^{n-1}l)(1+X)^{r'}(1+X)^{p^{n-1}l}\right)$$

$$= \sum_{r'=0}^{p^{n-1}-1} \mu_{n-1}(r')(1+X)^{r'}$$

$$= f_{n-1}(X)$$

となるので，(f_n) は射影極限 $\varprojlim \Lambda/\Lambda_n$ の元になる．この射影極限については，次の同型が成り立つ．

$$\Lambda \cong \varprojlim \Lambda/\Lambda_n \qquad (\Lambda \ni g \longmapsto (g_n) \in \varprojlim \Lambda/\Lambda_n).$$

ただし，$g \in \Lambda$ に対し，(g_n) は $g_n = g \bmod \Lambda_n$ で与えられる．これによって，上の $\{f_n\}$ から $f \in \Lambda$ は次のように与えられる．

$$f(X) = \sum_{k=0}^{\infty} c_k X^k,$$

ここで，

$$c_k = \lim_{n\to\infty} \sum_{r=0}^{p^n-1} \mu_n(r)\binom{r}{k}$$

$$= \int_{\mathbf{Z}_p} \binom{x}{k} d\mu(x).$$

重要なことは，$\mathcal{M}(\mathbf{Z}_p, \mathcal{O}_p)$ と形式的べき級数環 $\mathcal{O}_p[[X]]$ との間に岩澤同型と呼ばれる自然な同型が存在することである．

$f = \sum_{m=0}^{\infty} c_m X^m \in \mathcal{O}_p[[X]]$ に対し，$\mu = \{\mu_n\}$ を

$$\mu_n(r) = \frac{1}{p^n} \sum_{\zeta^{p^n}=1} \zeta^{-r} f(\zeta - 1) \qquad (r \in X_n) \tag{11.1}$$

で定義する．和は，ζ が 1 の p^n 乗根全体をわたることを意味する．$|\zeta - 1| < 1$ であるので，$f(\zeta - 1)$ は有限な値をもつ．各 $m \geq 0$ に対し

$$\frac{1}{p^n} \sum_{\zeta^{p^n}=1} \zeta^{-r} (\zeta - 1)^m = \frac{1}{p^n} \sum_{\zeta^{p^n}=1} \sum_{j=0}^{m} \zeta^{-r} \binom{m}{j} (-1)^{m-j} \zeta^j$$

$$= \sum_{\substack{0 \leq j \leq m \\ j \equiv r \bmod p^n}} \binom{m}{j} (-1)^{m-j}.$$

ζ を 1 の原始 p^ν 乗根 $(\nu \geq 1)$ とすれば

$$|\zeta - 1|^{\varphi(p^\nu)} = |p| \qquad (\varphi \text{ はオイラー関数})$$

であるので，

$$|(\zeta - 1)^m| = |p^{m/\varphi(p^\nu)}|$$

となる（$\varphi(p^\nu) = p^{\nu-1}(p-1)$）．よって上の式の左辺をながめると，右辺の値

$$\sum_{\substack{j \\ j \equiv r \bmod p^n}} \binom{m}{j} (-1)^{m-j}$$

は，$p^{m/\varphi(p^n)-n}$ 以上の p べきで割れる．したがって

$$\mu_n(r) = \sum_{m=0}^{\infty} c_m \left(\frac{1}{p^n} \sum_{\zeta^{p^n}=1} \zeta^{-r} (\zeta - 1)^m \right)$$

は収束し，$\mathcal{O}_p$ 値であることもわかる．測度の性質 (ii) を確かめるために

$$\sum_{y \in X_{n+1},\ \pi_{n+1}(y)=x} \mu_{n+1}(y) = \sum_{a \bmod p} \mu_{n+1}(x + p^n a)$$

$$= \frac{1}{p^{n+1}} \sum_{\zeta^{p^{n+1}}=1} \sum_{a \bmod p} \zeta^{-(x+p^n a)} f(\zeta - 1)$$

を計算すればよいのだが，1 の p^{n+1} 乗根 ζ については

$$\sum_{a \bmod p} \zeta^{-p^n a} = \begin{cases} 0 & \zeta^{p^n} \neq 1 \text{ のとき}, \\ p & \zeta^{p^n} = 1 \text{ のとき} \end{cases}$$

となることを使えば，

$$\sum_{y \in X_{n+1},\ \pi_{n+1}(y)=x} \mu_{n+1}(y) = \mu_n(x)$$

が従う．

以上，$\mathcal{M}(\mathbf{Z}_p, \mathcal{O}_p)$ と $\mathcal{O}_p[[X]]$ の間の対応を説明したが，より正確に次の定理が成り立つ．完全な証明は省略するが，Lang [59, Ch.4] などを参照されたい．

$\mathcal{M}(\mathbf{Z}_p, \mathcal{O}_p)$ の 2 つの測度 μ, ν に対し，たたみ込み積 $\mu * \nu$ の定義をする．

$$(\mu * \nu)_n(x) = \sum_{y=0}^{p^n-1} \mu_n(y)\nu_n(x-y) \qquad (x \in X_n). \tag{11.2}$$

このとき，$\mu * \nu = \{(\mu * \nu)_n\} \in \mathcal{M}(\mathbf{Z}_p, \mathcal{O}_p)$ となる．$\mathcal{M}(\mathbf{Z}_p, \mathcal{O}_p)$ はこのたたみ込み積 $\mu * \nu$ により $\mathcal{O}_p$ 代数になる．

定理 11.3（岩澤同型）$\mathcal{O}_p$ 値測度の空間 $\mathcal{M}(\mathbf{Z}_p, \mathcal{O}_p)$ と形式的べき級数環 $\mathcal{O}_p[[X]]$ の間には $\mathcal{O}_p$ 代数の同型 $P : \mathcal{M}(\mathbf{Z}_p, \mathcal{O}_p) \longrightarrow \mathcal{O}_p[[X]]$

$$\mathcal{M}(\mathbf{Z}_p, \mathcal{O}_p) \ni \mu = \{\mu_n\} \overset{P}{\longmapsto} f(X) = \sum_{n=0}^{\infty} c_n X^n \in \mathcal{O}_p[[X]]$$

が成り立つ．ここで，μ から f は

$$c_k = \int_{\mathbf{Z}_p} \binom{x}{k} d\mu(x)$$

で与えられ，逆に f から μ は

$$\mu_n(x) = \frac{1}{p^n} \sum_{\zeta^{p^n}=1} \zeta^{-x} f(\zeta - 1)$$

で復元される．

測度とべき級数との間の対応 P のいくつかの便利な性質を述べる．

以下の記述の便宜上 $\mathbf{Z}_p$ 上の $\mathcal{O}_p$ 値関数が連続になるための必要十分条件を与えるマーラー[1] の定理を掲げる．

定理 11.4　関数 $\varphi : \mathbf{Z}_p \longrightarrow \mathcal{O}_p$ が連続となるための必要十分条件は

$$\varphi(x) = \sum_{n=0}^{\infty} a_n \binom{x}{n}, \qquad a_n \in \mathcal{O}_p, \quad |a_n| \longrightarrow 0$$

[1]Kurt Mahler (1903.7.26 ドイツ Krefeld 生——1988.2.25 オーストラリア Canberra 没)

と書けることである．このとき，係数 a_n は φ から一意的に定まる．

定理の証明は省略する（Washington [88, §5.1] 参照）．

$\mathcal{O}_p$ の極大イデアルを

$$\mathcal{P} = \{z \in \mathcal{O}_p \mid |z| < 1\}$$

とおく．$z \in \mathcal{P}$ のとき x の関数 $(1+z)^x$ を

$$(1+z)^x := \sum_{n=0}^{\infty} \binom{x}{n} z^n$$

で定義すると，これはマーラーの定理により，$\mathbf{Z}_p$ 上の x の連続関数になる．x が非負整数のときは，$(1+z)^x$ の定義は通常の 2 項展開に一致する．この関数については，次の関係式が成り立つ．

$$(1+z)^x(1+z)^{x'} = (1+z)^{x+x'} \qquad (x,\ x' \in \mathbf{Z}_p). \tag{11.3}$$

この証明は，$x,\ x' \in \mathbf{N}$ のときは明らかであり，自然数の集合 $\mathbf{N}$ は $\mathbf{Z}_p$ の中で稠密であるから任意の $x,\ x' \in \mathbf{Z}_p$ について成立する．

性質 1)　$z \in \mathcal{P}$ とする．μ と f が対応しているとき（$P\mu = f$），

$$f(z) = \int_{\mathbf{Z}_p} (1+z)^x \, d\mu(x).$$

特に，$z = 0$ とすると

$$f(0) = \int_{\mathbf{Z}_p} d\mu(x).$$

証明　なぜなら，$f(X) = \sum_{n=0}^{\infty} c_n X^n$ と書くとき定理 11.3 より

$$\begin{aligned}\int_{\mathbf{Z}_p} (1+z)^x \, d\mu(x) &= \int_{\mathbf{Z}_p} \sum_{n=0}^{\infty} \binom{x}{n} z^n \, d\mu(x) \\ &= \sum_{n=0}^{\infty} z^n \int_{\mathbf{Z}_p} \binom{x}{n} d\mu(x) \\ &= \sum_{n=0}^{\infty} c_n z^n = f(z)\end{aligned}$$

となるからである．∎

$C(\mathbf{Z}_p, \mathcal{O}_p)$ から $\mathcal{O}_p$ への写像 λ が $C(\mathbf{Z}_p, \mathcal{O}_p)$ 上の有界線形汎関数であるとは

次の (i)，(ii) を満たすときをいう．

（i）　任意の $\varphi,\ \varphi' \in C(\mathbf{Z}_p, \mathcal{O}_p),\ a,\ b \in \mathcal{O}_p$ に対し

$$\lambda(a\varphi + b\varphi') = a\lambda(\varphi) + b\lambda(\varphi').$$

（ii）　ある正定数 $M > 0$ が存在し，任意の $\varphi \in C(\mathbf{Z}_p, \mathcal{O}_p)$ に対し，

$$|\lambda(\varphi)| \leq M\|\varphi\|.$$

λ のノルムは

$$\|\lambda\| = \max_{\substack{\varphi \in C(\mathbf{Z}_p, \mathcal{O}_p) \\ \varphi \neq 0}} \frac{|\lambda(\varphi)|}{\|\varphi\|}$$

で定義される．$C(\mathbf{Z}_p, \mathcal{O}_p)$ 上の有界線形汎関数 λ が与えられたとき，$x \in X_n = \mathbf{Z}/p^n\mathbf{Z}$ に対し，$x + p^n\mathbf{Z}_p$ の特性関数を $\varphi_{x,n}$ と書き，

$$\mu_n(x) = \lambda(\varphi_{x,n})$$

とおくと，$\mu = \{\mu_n\}$ は $\mathbf{Z}_p$ 上の $\mathcal{O}_p$ 値測度（$\mu \in \mathcal{M}(\mathbf{Z}_p, \mathcal{O}_p)$）になる．逆に $\mu = \{\mu_n\} \in \mathcal{M}(\mathbf{Z}_p, \mathcal{O}_p)$ に対しては

$$\lambda(\varphi) = \int_{\mathbf{Z}_p} \varphi(x)\,d\mu(x)$$

とすれば，λ は $C(\mathbf{Z}_p, \mathcal{O}_p)$ 上の有界線形汎関数になる．この λ と μ の対応は，容易に示すことができるように 1 対 1 である．

さらに，$h \in C(\mathbf{Z}_p, \mathcal{O}_p)$ と測度 $\mu \in \mathcal{M}(\mathbf{Z}_p, \mathcal{O}_p)$ から，写像

$$\varphi \longmapsto \int_{\mathbf{Z}_p} \varphi(x)h(x)\,d\mu(x) \qquad (\varphi \in C(\mathbf{Z}_p, \mathcal{O}_p))$$

を考えると，$C(\mathbf{Z}_p, \mathcal{O}_p)$ 上の有界線形汎関数になる．これに対応する測度を $h\mu$ と記す．μ が $f \in \mathcal{O}_p[[X]]$ と対応するとき（$P\mu = f$），測度 $h\mu$ に対応する形式的べき級数を求めるのは興味深い問題である．以下で述べる性質 2)，3) がこのことの好例を与えている．

$f \in \mathcal{O}_p[[X]]$ に対し

$$(\mathbb{U}f)(X) = f(X) - \frac{1}{p}\sum_{\zeta^p=1} f(\zeta(1+X)-1) \tag{11.4}$$

とおく．各非負整数 l に対して

$$\frac{1}{p}\sum_{\zeta^p=1} (\zeta(1+X)-1)^l \in \mathbf{Z}_p[X]$$

であるから，$\mathbb{U}f \in \mathcal{O}_p[[X]]$ である．

性質 2)　$f \in \mathcal{O}_p[[X]]$ とし，対応する測度を μ_f で表す．また ψ を $\mathbf{Z}_p^\times$ の特性関数とする．このとき，測度 $\psi\mu_f$ に対応する形式的べき級数は $\mathbb{U}f$ である，すなわち $\psi\mu_f = \mu_{\mathbb{U}f}$ である．詳しく書くと，任意の $\varphi \in C(\mathbf{Z}_p, \mathcal{O}_p)$ に対し，

$$\int_{\mathbf{Z}_p} \varphi(x)\psi(x)\,d\mu_f(x) = \int_{\mathbf{Z}_p} \varphi(x)\,d\mu_{\mathbb{U}f}(x)$$

となる．これはまた

$$\int_{\mathbf{Z}_p^\times} \varphi(x)\,d\mu_f(x) = \int_{\mathbf{Z}_p} \varphi(x)\,d\mu_{\mathbb{U}f}(x)$$

とも書ける．

証明　測度 $\psi\mu_f$ に対応する形式的べき級数を g と書くと，$z \in \mathcal{P}$ のとき，性質 1) より

$$g(z) = \int_{\mathbf{Z}_p} (1+z)^x \psi(x)\,d\mu_f(x).$$

ζ を 1 の p 乗根とする．$\psi(a \bmod p) = \psi(a + p\mathbf{Z}_p)$ により，ψ を $\mathbf{Z}/p\mathbf{Z}$ 上の関数とも見なし，

$$\widehat{\psi}(\zeta) = \frac{1}{p} \sum_{a \in \mathbf{Z}/p\mathbf{Z}} \psi(a)\zeta^{-a} \qquad (\mathbf{Z}/p\mathbf{Z} \text{ 上のフーリエ変換})$$

とおくと，簡単な計算により

$$\psi(a) = \sum_{\zeta^p = 1} \widehat{\psi}(\zeta)\zeta^a \qquad (\text{フーリエ逆変換})$$

となる．ψ の定義より，

$$\widehat{\psi}(\zeta) = \begin{cases} -\frac{1}{p} & \zeta \neq 1 \text{ のとき}, \\ \frac{p-1}{p} & \zeta = 1 \text{ のとき} \end{cases}$$

となるので，

$$
\begin{aligned}
g(z) &= \int_{\mathbf{Z}_p} (1+z)^x \psi(x)\, d\mu_f(x) \\
&= \int_{\mathbf{Z}_p} (1+z)^x \sum_{\zeta^p=1} \widehat{\psi}(\zeta)\zeta^x\, d\mu_f(x) \\
&= \sum_{\zeta^p=1} \widehat{\psi}(\zeta) \int_{\mathbf{Z}_p} (1+z)^x \zeta^x\, d\mu_f(x) \\
&= \sum_{\zeta^p=1} \widehat{\psi}(\zeta) \int_{\mathbf{Z}_p} \Big(1+(\zeta(1+z)-1)\Big)^x d\mu_f(x) \\
&= \sum_{\zeta^p=1} \widehat{\psi}(\zeta) f(\zeta(1+z)-1) \\
&= f(z) - \frac{1}{p} \sum_{\zeta^p=1} f(\zeta(1+z)-1)
\end{aligned}
$$

が得られる．ここで $x \in \mathbf{Z}_p$ に対する ζ^x は，

$$
\zeta^x = (1+\zeta-1)^x = \sum_{n=0}^{\infty} \binom{x}{n} (\zeta-1)^n
$$

で定義する．$x - a \in p\mathbf{Z}_p$ なる $a \in \mathbf{Z}$ を選べば，$\zeta^x = \zeta^a$ となる．これより，$g = \mathbb{U}f$. ∎

形式的べき級数環 $\mathcal{O}_p[[X]]$ 上の微分作用素 D を

$$
D = (1+X)D_X, \qquad \text{ただし} \quad D_X = \frac{d}{dX}
$$

で定義する．

性質 3)　$f \in \mathcal{O}_p[[X]]$ に対し，測度 $x\mu_f$ に対応するべき級数は Df である．したがって，測度 $x^k\mu_f$（k は自然数）に対応するべき級数は $D^k f$ であり，

$$
\int_{\mathbf{Z}_p} x^k\, d\mu_f(x) = \int_{\mathbf{Z}_p} d\mu_{D^k f}(x) = (D^k f)(0)
$$

となる．

証明　$k = 1$ のときを示せば十分である．測度 $x\mu_f$ に対応するべき級数を $g \in \mathcal{O}_p[[X]]$ とする．性質 1) より $z \in \mathcal{P}$ に対し，

$$g(z) = \int_{\mathbf{Z}_p} x(1+z)^x \, d\mu_f(x).$$

いま，$f(X) = \sum_{n=0}^{\infty} a_n X^n$，$g(X) = \sum_{n=0}^{\infty} b_n X^n$ とすると，2 項多項式 $\binom{X}{n}$ について

$$X\binom{X}{n} = (n+1)\binom{X}{n+1} + n\binom{X}{n}$$

であるので，定理 11.3 を用いて

$$\begin{aligned} b_n &= \int_{\mathbf{Z}_p} \binom{x}{n} d\mu_g(x) = \int_{\mathbf{Z}_p} \binom{x}{n} x \, d\mu_f(x) \\ &= (n+1)\int_{\mathbf{Z}_p} \binom{x}{n+1} d\mu_f(x) + n\int_{\mathbf{Z}_p} \binom{x}{n} d\mu_f(x) \\ &= (n+1)a_{n+1} + na_n. \end{aligned}$$

一方，Df を計算すると，

$$\begin{aligned} (Df)(X) &= ((1+X)D_X f)(X) \\ &= (1+X)(a_1 + 2a_2X + \cdots + na_nX^{n-1} + \cdots) \\ &= \sum_{n=0}^{\infty} ((n+1)a_{n+1} + na_n)X^n \end{aligned}$$

となるので，$g = Df$ が従う． ■

一般に，形式的べき級数 $f(X)$ に対して，新たな形式的べき級数 $f^*(Z)$ を $X = e^Z - 1$ とおくことにより

$$f^*(Z) = f(e^Z - 1) \tag{11.5}$$

で定義する．たとえば

$$f(X) = (1+X)^a = \sum_{n=0}^{\infty} \binom{a}{n} X^n$$

であるときは，

$$f^*(Z) = e^{aZ} = \sum_{n=0}^{\infty} \frac{a^n Z^n}{n!}$$

となる．一般に

$$D_Z f^*(Z) = (1+X)D_X f(X) = Df(X)$$

となるので，

$$(D_Z^k f^*)(0) = (D^k f)(0) \tag{11.6}$$

が成り立つことに注意する．

次の性質が定理 11.3 の同型 P が $\mathcal{O}_p$ 代数としての同型になる基礎となる．

性質 4)　測度 μ, ν はそれぞれ，形式的べき級数 f, $g \in \mathcal{O}_p[[X]]$ に対応しているとする（すなわち，$\mu = \mu_f$, $\nu = \mu_g$）．このとき，たたみ込み積による測度 $\mu * \nu$ に対応する形式的べき級数は fg である．すなわち，

$$\mu_f * \mu_g = \mu_{fg}.$$

証明　(11.1) 式により

$$\mu_n(r) = \frac{1}{p^n} \sum_{\zeta^{p^n}=1} \zeta^{-r} f(\zeta - 1),$$

$$\nu_n(k-r) = \frac{1}{p^n} \sum_{\zeta^{p^n}=1} \zeta^{-k+r} g(\zeta - 1).$$

このとき，(11.2) 式の右辺に上の式を代入して多少変形すると

$$\begin{aligned}
(\mu * \nu)_n(k) &= \sum_{r=0}^{p^n-1} \frac{1}{p^n} \sum_{\zeta^{p^n}=1} \zeta^{-r} f(\zeta - 1) \frac{1}{p^n} \sum_{\xi^{p^n}=1} \xi^{-k+r} g(\xi - 1) \\
&= \frac{1}{p^n} \sum_{\zeta} \sum_{\xi} f(\zeta - 1) g(\xi - 1) \xi^{-k} \cdot \frac{1}{p^n} \sum_{r=0}^{p^n-1} (\xi/\zeta)^r \\
&= \frac{1}{p^n} \sum_{\zeta} f(\zeta - 1) g(\zeta - 1) \zeta^{-k} \\
&= \mu_{fg,\,n}(k)
\end{aligned}$$

となる．ここで，ζ と ξ は 1 の p^n 乗根全体をわたる．これより，性質 4) が従う． ∎

11.2　ベルヌーイ測度

この節の目標であるベルヌーイ測度を定義する．

$$B_1(x) = x - \frac{1}{2}$$

であることを思い出そう．以下，p は奇素数とする．

各 n と $x \in X_n = \mathbf{Z}/p^n\mathbf{Z}$（代表 x は $x \in \mathbf{Z}$ にとる）に対し

$$E_n(x) = B_1\left(\left\{\frac{x}{p^n}\right\}\right)$$

とおく．ただし $w \in \mathbf{R}$ に対し，$\{w\}$ は $0 \leq \{w\} < 1$ かつ $w - \{w\} \in \mathbf{Z}$ を満たす実数とする（w の小数部分）．$E = \{E_n\}$ は $\mathbf{Z}_p$ 上の測度になるが $\mathcal{O}_p$ 値ではない．$\mathcal{O}_p$ 値にするために次の工夫をする．$\mathbf{Z}_p$ の可逆元 $c(c \in \mathbf{Z}_p^{\times})$ をとり，$x \in X_n = \mathbf{Z}/p^n\mathbf{Z}$ に対し

$$E_{c,n}(x) = E_n(x) - cE_n(c^{-1}x)$$

とおく．ただし $c^{-1}x$ は $X_n = \mathbf{Z}/p^n\mathbf{Z}$ の元として理解する．$E_c = \{E_{c,n}\}$ は $\mathcal{O}_p$ 値測度になる．これをベルヌーイ測度と呼ぶ．

命題 11.5

（1） ベルヌーイ測度 E_c に対応するべき級数は

$$f_c(X) = \frac{1}{X} - \frac{c}{(1+X)^c - 1}$$

である．

（2） $c \in \mathbf{Z}_p^{\times}$ かつ $c^k \neq 1$ とすると

$$\frac{B_k}{k} = \frac{(-1)^k}{1-c^k}\int_{\mathbf{Z}_p} x^{k-1}\, dE_c.$$

証明 (1) $c \in \mathbf{Z}_p^{\times}$ であるので，$f_c \in \mathbf{Z}_p[[X]]$ がわかる．$f_c(X)$ のべき級数展開の最初の 2 項は

$$f_c(X) = \frac{c-1}{2} + \frac{1-c^2}{12}X + \cdots$$

で与えられる．定理 11.3 により f_c に対応する $\mathbf{Z}_p$ 上の測度を $\mu = \{\mu_n\}$ とする．$k \in X_n = \mathbf{Z}/p^n\mathbf{Z}$ に対して

$$\mu_n(k) = \frac{1}{p^n} \sum_{\zeta^{p^n}=1} \zeta^{-k} f_c(\zeta - 1)$$

$$= \frac{1}{p^n} f_c(0) + \frac{1}{p^n} \sum_{\zeta^{p^n}=1,\, \zeta\neq 1} \zeta^{-k} \left(\frac{1}{\zeta - 1} - \frac{c}{\zeta^c - 1} \right).$$

ここで，112 ページ補題 8.5 を用いる．$\zeta^{p^n} = 1,\ \zeta \neq 1$ のとき，$f = p^n$ とおくと $(c,p) = 1$ より

$$\frac{1}{\zeta^c - 1} = \frac{1}{f} \sum_{j=1}^{f-1} j\zeta^{cj}$$

となる．よって，整数 l を $cl \equiv k \bmod p^n,\ 0 \leq l < p^n$ を満たすように選ぶと

$$\frac{1}{f} \sum_{\zeta^{p^n}=1,\, \zeta\neq 1} \zeta^{-k} \frac{c}{\zeta^c - 1} = \frac{c}{f^2} \sum_{\zeta^{p^n}=1} \zeta^{-k} \sum_{j=1}^{f-1} j\zeta^{cj} - \frac{c(f-1)}{2f}$$

$$= \frac{cl}{f} - \frac{c(f-1)}{2f}$$

$$= c\left\{ \frac{c^{-1}k}{p^n} \right\} - \frac{c}{2} + \frac{c}{2f}$$

となり，$\mu_n(k)$ の式に代入して（$f_c(0) = (c-1)/2$ に注意して）

$$\mu_n(k) = \frac{c-1}{2f} + \left(\left\{ \frac{k}{p^n} \right\} - \frac{1}{2} + \frac{1}{2f} - c\left\{ \frac{c^{-1}k}{p^n} \right\} + \frac{c}{2} - \frac{c}{2f} \right)$$

$$= \left(\left\{ \frac{k}{p^n} \right\} - \frac{1}{2} \right) - c\left(\left\{ \frac{c^{-1}k}{p^n} \right\} - \frac{1}{2} \right)$$

となるので，ベルヌーイ測度の定義より $\mu_n(k) = E_{c,n}(k)$，すなわち，$\mu = E_c$ が従い，E_c に対応する形式的べき級数は f_c である．

(2) は次のようにする．性質 3) と (11.6) 式により

$$\int_{\mathbf{Z}_p} x^{k-1}\, dE_c = (D^{k-1} f_c)(0) = (D_Z^{k-1} f_c^*)(0)$$

である．f_c^* は (11.5) 式より

$$f_c^*(Z) = f_c(e^Z - 1) = \frac{1}{e^Z - 1} - \frac{c}{e^{cZ} - 1}$$

$$= \sum_{n=1}^{\infty} (1 - c^n)(-1)^n B_n \frac{Z^{n-1}}{n!}$$

であるから，

$$(D_Z^{k-1} f_c^*)(0) = (1 - c^k)(-1)^k \frac{B_k}{k}$$

となる．よって

$$\int_{\mathbf{Z}_p} x^{k-1}\, dE_c = (1 - c^k)(-1)^k \frac{B_k}{k}.$$

これより，(2) が従う． ∎

11.3 クンマー合同式再論

クンマー合同式の「正しい」定式化は次のとおりである．

定理 11.6 p を奇素数とし，a を 1 以上の整数，m, n を正の偶数で，$m \equiv n \bmod (p-1)p^{a-1}$ かつ $m \not\equiv 0 \bmod (p-1)$ を満たすものとする．このとき，

$$(1 - p^{m-1})\frac{B_m}{m} \equiv (1 - p^{n-1})\frac{B_n}{n} \mod p^a$$

が成り立つ．

この定理の証明の基礎になる，次のベルヌーイ数の積分表示をまず証明する．(命題 11.5 (2) の積分表示では定理の形のクンマー合同式を証明するには不十分である．)

命題 11.7 k は正の偶数とし，$c \in \mathbf{Z}$ かつ $(c, p) = 1$ とする（$c \in \mathbf{Z}_p^\times$ でよい）．このとき，積分表示

$$(1 - c^k)(1 - p^{k-1})\frac{B_k}{k} = \int_{\mathbf{Z}_p^\times} x^{k-1}\, dE_c$$

が成り立つ．

証明 ベルヌーイ測度 E_c に対応するべき級数は，命題 11.5 の f_c であった．f_c から (11.4) 式に従って新しいべき級数 g を

$$g(X) = \mathbb{U} f_c(X) = f_c(X) - \frac{1}{p} \sum_{\zeta^p = 1} f_c(\zeta(1+X) - 1)$$

で定義する．$g \in \mathcal{O}_p[[X]]$ であり，g から得られる $\mathcal{O}_p$ 値測度を $\mu = \mu_g$ とする．性質 2) により

$$\int_{\mathbf{Z}_p^\times} x^{k-1}\, dE_c = \int_{\mathbf{Z}_p} x^{k-1}\, d\mu$$

となる．さらに性質 3) と (11.6) 式を用いると

$$\int_{\mathbf{Z}_p} x^{k-1}\, d\mu = (D^{k-1} g)(0) = (D_Z^{k-1} g^*)(0).$$

命題の主張はこの値 $(D_Z^{k-1} g^*)(0)$ の計算に帰着する．$g^*(Z)$ を $g(X)$ から計算しよう．

$$g^*(Z) = \frac{1}{e^Z - 1} - \frac{c}{e^{cZ} - 1} - \frac{1}{p} \sum_{\zeta^p = 1} \left(\frac{1}{\zeta e^Z - 1} - \frac{c}{\zeta^c e^{cZ} - 1} \right),$$

ここで

$$\frac{1}{p} \sum_{\zeta^p = 1} \frac{1}{\zeta X - 1} = \frac{1}{X^p - 1}$$

であるので

$$\begin{aligned} g^*(Z) &= \frac{1}{e^Z - 1} - \frac{c}{e^{cZ} - 1} - \left(\frac{1}{e^{pZ} - 1} - \frac{c}{e^{cpZ} - 1} \right) \\ &= \sum_{k=0}^{\infty} (1 - c^k)(-1)^k \frac{B_k}{k!} Z^{k-1} - \sum_{k=0}^{\infty} (1 - c^k)(-1)^k \frac{B_k}{k!} (pZ)^{k-1} \\ &= \sum_{k=1}^{\infty} (1 - c^k)(1 - p^{k-1})(-1)^k \frac{B_k}{k!} Z^{k-1} \end{aligned}$$

となる．よって k が偶数のとき

$$(D_Z^{k-1} g^*)(0) = (1 - c^k)(1 - p^{k-1}) \frac{B_k}{k}$$

が得られ，証明が完了する．　■

定理 11.6 の証明　$c \in \mathbf{Z}$ を $(c, p) = 1$，$c^m \not\equiv 1 \bmod p$ にとる．たとえば c を $\bmod p$ の原始根にとればよい．命題 11.7 より

$$(1-c^n)(1-p^{n-1})\frac{B_n}{n} = \int_{\mathbf{Z}_p^\times} x^{n-1}\,dE_c$$

かつ

$$(1-c^m)(1-p^{m-1})\frac{B_m}{m} = \int_{\mathbf{Z}_p^\times} x^{m-1}\,dE_c$$

となる．仮定より $m \equiv n \bmod (p-1)p^{a-1}$ だから $c^{n-m} \equiv 1 \bmod p^a$ かつ，$p-1 \nmid n$ なので $(1-c^n, p) = 1$．また $x \in \mathbf{Z}_p^\times$ のとき $x^{m-1} \equiv x^{n-1} \bmod p^a$ であり，E_c は $\mathcal{O}_p$ 値測度であるから

$$(1-c^n)\left((1-p^{n-1})\frac{B_n}{n} - (1-p^{m-1})\frac{B_m}{m}\right) \in p^a\mathcal{O}_p$$

となるが，左辺は $\mathbf{Z}_p$ に含まれるから，結論として

$$\left((1-p^{n-1})\frac{B_n}{n} - (1-p^{m-1})\frac{B_m}{m}\right) \in p^a\mathbf{Z}_p.$$

これより定理が得られる． ∎

第12章

フルヴィッツ数

12.1 フルヴィッツ数

この節では Hurwitz が行ったベルヌーイ数の一般化についての研究を簡単に紹介する.

彼は，ベルヌーイ数は三角関数の展開係数であるという見方から，これを「レムニスケート（lemniscate）関数」に置き換えても，その展開係数は似たような数論的性質をもつに違いないと考え，実際それを示してみせたのである．レムニスケート関数とは，三角関数のある一般化であって，いまの言葉でいうとガウス整数環 $\mathbf{Z}[\sqrt{-1}]$ に虚数乗法をもつ楕円関数の 1 つである．最初にそのような関数を研究したのは Gauss であるが，彼はそれを生前公表することはなかった．しかし，その著 *Disquisitiones Arithmeticae*（数論考究 [27]，1801）の，円周等分の章（第 7 章）のはじめに，以下の自分の理論はレムニスケート[1]の等分の場合にも適用可能であることを示唆する記述を入れた．そのヒントをもとに楕円関数の理論を大きく構築発展させたのが Abel[2]と Jacobi である．

フルヴィッツ数を定義しよう．そのために，まず

$$\varpi = 2\int_0^1 \frac{dx}{\sqrt{1-x^4}}$$

[1]極座標で $r^2 = 2a^2\cos(2\theta)$ $(a>0)$ で定義される平面曲線，ちなみにこれを「Jakob Bernoulli のレムニスケート」と呼ぶことがある

[2]Niels Henrik Abel（1802.8.5 ノルウェー Frindoe 生——1829.4.6 ノルウェー Froland 没）

とおく．これはレムニスケート $r^2 = \cos(2\theta)$ の周長の半分であって，円周率が積分

$$\pi = 2\int_0^1 \frac{dx}{\sqrt{1-x^2}}$$

で表されることと対比させると，「レムニスケート周率」とでも呼びうる数である．次に，ϖ と $\varpi\sqrt{-1}$ を周期にもつワイエルシュトラスの楕円関数を $\wp(z)$ と書く[3]．これは無限級数で次のように定義される．

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{\lambda \in \mathbf{Z}\varpi + \mathbf{Z}\varpi\sqrt{-1} \\ \lambda \neq 0}} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right). \tag{12.1}$$

$\wp(z)$ は，複素平面において，格子 $\mathbf{Z}\varpi + \mathbf{Z}\varpi\sqrt{-1}$ 上の点でのみ 2 位の極をもちそれ以外では正則な複素関数で，z を $z+\lambda$ $(\lambda \in \mathbf{Z}\varpi + \mathbf{Z}\varpi\sqrt{-1})$ に置き換えても値がかわらないという 2 重周期性をもつ（三角関数の一般化）．この格子が $\sqrt{-1}$ 倍で保たれるということから，$\lambda \in \mathbf{Z}\varpi + \mathbf{Z}\varpi\sqrt{-1}$ に対して $\wp(\lambda z)$ が $\wp(z)$ と $\wp'(z)$ の有理式で表されることがわかる．この性質から，$\wp(z)$ は $\mathbf{Z}[\sqrt{-1}]$ を虚数乗法にもつ楕円関数であるといわれるのである．楕円関数というのは，楕円の周長の計算に現れる積分の逆関数を考えると，それがこういった 2 重周期関数になることに由来する名前である．

定義からわかるように $\wp(z)$ は偶関数であり，また，z，λ をともに $\sqrt{-1}$ 倍で置き換えてみると，$\mathbf{Z}\varpi + \mathbf{Z}\varpi\sqrt{-1}$ が $\sqrt{-1}$ 倍でかわらないことから，

$$\wp(\sqrt{-1}z) = -\wp(z)$$

が成り立つ．また，微分方程式

$$\wp'(z)^2 = 4\wp(z)^3 - 4\wp(z),$$

さらにこれを微分した

$$\wp''(z) = 6\wp(z)^2 - 2$$

を満たす[4]．

---

[3] 本来は $\wp(z; \mathbf{Z}\varpi + \mathbf{Z}\varpi\sqrt{-1})$ と書かれるべきものを略記する．なお，以下に述べる諸性質については [84] などを参照．

[4] ϖ を与える積分は変数変換 $x = \frac{1}{\sqrt{z}}$ により

$$\varpi = 2\int_1^\infty \frac{dz}{\sqrt{4z^3 - 4z}}$$

と書ける．このことから，慣用の記号で $g_2 = 4$，$g_3 = 0$ が導かれ，この微分方程式を得る．詳しくは [84] などを参照．

さて $\wp(z)$ の原点でのローラン展開を考える．定義からそれが $\frac{1}{z^2}+\cdots$ で始まることがわかるが，そのほかの係数を

$$\wp(z)=\frac{1}{z^2}+\sum_{n=2}^{\infty}\frac{2^nH_n}{n}\frac{z^{n-2}}{(n-2)!} \tag{12.2}$$

のように書く．すると上記 $\wp(-z)=\wp(z)$，$\wp(\sqrt{-1}z)=-\wp(z)$ より，H_n は $n=4,8,12,\cdots$（4 の倍数）のとき以外は零であることがわかる．このときの H_n がフルヴィッツ数と呼ばれるものである．三角関数と対比させるなら，

$$\frac{1}{\sin^2(x)}=\frac{1}{x^2}+\sum_{n=2}^{\infty}\frac{(-1)^{\frac{n}{2}-1}2^nB_n}{n}\frac{x^{n-2}}{(n-2)!}$$

という展開式がこれに対応する．これは，21 ページ命題 1.17 で与えた cot の展開式

$$\cot(x)=\frac{1}{x}+\sum_{n=1}^{\infty}(-1)^n2^{2n}B_{2n}\frac{x^{2n-1}}{(2n)!}$$

を微分して，$\cot'(x)=-\frac{1}{\sin^2(x)}$ を使うと得られる．20 ページ命題 1.15 の証明と同様に，微分方程式 $\wp''(z)=6\wp(z)^2-2$ の展開係数を比較することにより，

$$H_4=\frac{1}{10},$$

および，$n\geq 2$ に対し漸化式

$$(2n-3)(4n-1)(4n+1)H_{4n}=3\sum_{i=1}^{n-1}(4i-1)(4n-4i-1)\binom{4n}{4i}H_{4i}H_{4(n-i)}$$

が得られる．これから，H_{4n} は正の有理数であることがわかる．いくつかの値を表にしておこう．

表 12.1: フルヴィッツ数

n	4	8	12	16	20	24	28	32
H_n	$\frac{1}{10}$	$\frac{3}{10}$	$\frac{567}{130}$	$\frac{43659}{170}$	$\frac{392931}{10}$	$\frac{1724574159}{130}$	$\frac{2498907956391}{290}$	$\frac{1671769422825579}{170}$

フルヴィッツ数とベルヌーイ数の類似性はゼータ関数の特殊値について見るとよりはっきりする．すなわち，まず公式 (4.4)（61 ページ）を

$$\sum_{r\in\mathbf{Z}\setminus\{0\}}\frac{1}{r^{2n}}=(-1)^{n-1}\frac{(2\pi)^{2n}}{(2n)!}B_{2n}\qquad(n\geq 1)$$

と書く．左辺は 0 以外のすべての整数をわたっている．この左辺のかわりに，有理整数をガウスの整数（$\mathbf{Q}(\sqrt{-1})$ の極大整環 $\mathbf{Z}[\sqrt{-1}]$ の元）で置き換えて逆数のべきの和をとったものにすると，

$$\sum_{\substack{\lambda \in \mathbf{Z}+\mathbf{Z}\sqrt{-1} \\ \lambda \neq 0}} \frac{1}{\lambda^{4n}} = \frac{(2\varpi)^{4n}}{(4n)!} H_{4n}$$

が成り立つのである．これは，$\wp(z)$ の定義式 (12.1) の右辺を $\frac{1}{(z-\lambda)^2} = \frac{1}{\lambda^2} + \frac{2z}{\lambda^3} + \frac{3z^2}{\lambda^4} + \cdots$ を用いて展開したものと H_n の定義式 (12.2) を比較すると得られる．

Hurwitz はこの H_n に対してクラウゼン・フォンシュタウトの定理の類似を証明した．それを述べるために次のフェルマー[5]・オイラーの定理が必要になる．

定理 12.1　4 で割って 1 余る素数は平方数の和として本質的に 1 通りに表される

証明　この定理はさまざまな証明が知られており，ガウス整数環における有理素数の分解定理（158 ページ定理 10.11）としてとらえるのが最も自然であるが，ここでは，平方和分解の存在証明として，Heath-Brown の証明を簡易化した Zagier による “One-sentence proof” [95] を紹介しよう．一文で書くと

「有限集合 $S = \left\{(x,y,z) \in \mathbf{N}^3 : x^2 + 4yz = p\right\}$ 上，

$$(x,y,z) \mapsto \begin{cases} (x+2z, z, y-x-z) & x < y-z \text{ のとき}, \\ (2y-x, y, x-y+z) & y-z < x < 2y \text{ のとき}, \\ (x-2y, x-y+z, y) & x > 2y \text{ のとき} \end{cases}$$

で定義される involution はただ 1 つの固定点をもつので，S の位数は奇数であり，したがって $(x,y,z) \mapsto (x,z,y)$ で定義される involution も固定点をもつ．」

もう少し説明すると，まず S が有限集合であることはよい．そして，上で定義される写像が involution，つまり 2 回繰り返すと恒等写像になる（特に involution は全単射）ことは定義に従って確かめることができる．また，p は 4 で割って

[5]Pierre de Fermat（1601.8.17 フランス Beaumont-de-Lomagne 生――1665.1.12 フランス Castres 没）

1 余るからこれを $4k+1$ と書くと，$(1,1,k)$ が唯一の固定点になる．(3 つの場合分けのうち，第 1，第 3 の場合は，x の値がかわるので固定点になり得ない．第 2 の場合，$x=y$ が固定点の条件だが，このとき $x^2+4xz=p$ となり，p は素数なので $x=1$ である．) すると，固定点以外はこの involution でペアになるので，S の元の個数は奇数である．すると，$(x,y,z)\mapsto(x,z,y)$ が S 上の involution であることは明らかなので，これによってうつりあうものを組にしていくと，必ず固定点が存在しなくてはならないことになる．すなわち (x,y,y) の形の元が S に存在して，このとき $p=x^2+4y^2=x^2+(2y)^2$ である．

次に，表し方が本質的に 1 通り，ということであるが，それはたとえば次のようにする．

$$p=a^2+b^2=c^2+d^2$$

と 2 通りに表されたとしよう．a,b,c,d は正整数としてよい．明らかに $1\le a,b,c,d<p$ である．この表示を $\bmod p$ で考える．p は 4 で割ると 1 余る素数であるから，合同式 $x^2\equiv -1 \pmod p$ の解は 2 つであり，$\frac{a}{b}$ と $\frac{b}{a}$，また $\frac{c}{d}$ と $\frac{d}{c}$ がそれら 2 つの解を与えている．$\frac{a}{b}\equiv\frac{b}{a} \pmod p$ ということは起こらない．なぜならこのとき $a^2\equiv b^2 \pmod p$ となり $0\equiv a^2+b^2\equiv 2a^2 \pmod p$ となるが，2 も a も p で割れないからこれは矛盾である．同様に $\frac{c}{d} \bmod p$ と $\frac{d}{c} \bmod p$ も異なる．したがって，$\frac{a}{b}\equiv\frac{c}{d} \pmod p$ または $\frac{a}{b}\equiv\frac{d}{c} \pmod p$ である．前者であると仮定しても一般性を失わないからそうすると，$ad-bc$ が p の倍数ということになる．ところが

$$p^2=(a^2+b^2)(c^2+d^2)=(ad-bc)^2+(ac+bd)^2$$

という式が成り立つので，$ac+bd>0$ より $|ad-bc|<p$，よって $ad-bc=0$ でなければならない．すると $ad=bc$ より，$\frac{a}{c}=\frac{b}{d}$．これを k とおくと $a=kc, b=kd$．$a^2+b^2=c^2+d^2$ より $k^2=1$，よって $k=1$ となり，$a=c, b=d$ である． ∎

いま p を 4 で割ると 1 余る素数とし，その平方和への分解を

$$p=a^2+b^2$$

とする．このとき a,b のいずれか一方のみが奇数でなくてはならないからそれを a とし，その符号を

$$a\equiv b+1 \mod 4$$

で定める．これで a は一意的に決まる (偶数 b の $\bmod 4$ での類は符号の取り方

によらず定まるから）．このように定まる a を，p を明示して a_p と書くことにする．このときフルヴィッツの定理は次のとおり．

定理 12.2　各 $n \geq 1$ に対してある整数 G_n があって，

$$H_{4n} = \frac{1}{2} + \sum_{\substack{p \equiv 1 \bmod 4 \\ p-1 \mid 4n}} \frac{(2a_p)^{\frac{4n}{p-1}}}{p} + G_n.$$

p は 4 で割ると 1 余る素数で $p-1$ が $4n$ を割るようなものを動く．

例として，

$$\begin{aligned}
H_4 &= \frac{1}{10} = \frac{1}{2} - \frac{2}{5}, \\
H_8 &= \frac{3}{10} = \frac{1}{2} + \frac{2^2}{5} - 1, \\
H_{12} &= \frac{567}{130} = \frac{1}{2} - \frac{2^3}{5} + \frac{6}{13} + 5, \\
H_{16} &= \frac{43659}{170} = \frac{1}{2} + \frac{2^4}{5} + \frac{2}{17} + 253, \\
H_{20} &= \frac{392931}{10} = \frac{1}{2} - \frac{2^5}{5} + 39299, \\
H_{24} &= \frac{1724574159}{130} = \frac{1}{2} + \frac{2^6}{5} + \frac{6^2}{13} + 13265939
\end{aligned}$$

など．Hurwitz は G_n が $n=1$ のとき以外はすべて奇数であることや，その 8 で割った剰余を完全に決定する命題も証明している．

定理の証明はベルヌーイ数のクラウゼン・フォンシュタウトの定理ほど簡単ではなく，$\wp$ 関数の虚数乗法とフルヴィッツ整級数の概念を巧みに用いてなされる [37]．この定理の現代的な解釈，また，クンマー合同式の類似については [21]，[51] を参照していただきたい．

12.2　フルヴィッツ小伝

Adolf Hurwitz は 1859 年 3 月 26 日，ドイツの Hildesheim の生まれである[6]．地元のギムナジウムの教師に，数え上げ幾何の「シューベルト算法」で有名な

[6] 以下の記述は Freudenthal [26]，Hilbert [32]，Meissner [63] に基づく．

Schubert[7]がいた．Schubert は Hurwitz の才能に注目，日曜日ごとに家庭教師をし，必ずしも裕福ではなかった彼の父親を説得し大学で数学を学ぶ道を進ませた．Hurwitz はすでにギムナジウム在学中，17 才のときに Schubert と共著で数え上げ幾何に関する論文を書いている．1877 年の春に Klein[8]のいた München 工科大学に入学，同じ年の秋から 1879 年の春までは Berlin 大学にいて Kummer, Weierstrass, Kronecker らの講義を聞いた．その後再び München に戻り，Klein が Leipzig に移るとともに Leipzig に行き，そこでモジュラー関数に関する研究で博士号をとった．1882 年に Göttingen 大学の私講師（Privatdozent），そして 1884 年，Lindemann[9]の招きで Königsberg 大学の教授となる．そこでの学生に Hilbert[10]や Minkowski[11]がいた．若き日の彼ら 3 人の交流の様子，Hilbert が彼らからいかに影響を受けたかなどが，[70] に生き生きと描かれている．1892 年，Frobenius[12]の後継として，スイスの Zürich 工科大学に赴任，終生をそこで過ごした．同時期，Berlin に移った Schwarz の後継として Göttingen からも招聘があったが，すでに Zürich を受諾した後であった．（当時の Zürich の視学官長 Bleuler という人が Königsberg まで出向いて契約を交したという．）

Hurwitz は身体が丈夫ではなかった．腸チフスに 2 度かかり，偏頭痛にしばしば悩まされた．また 1905 年には片方の腎臓を摘出している．そのような中で研究を続け，広い分野にまたがって多くの仕事をした．その論文は 2 巻の全集に収められている．この本で扱ったフルヴィッツゼータ関数，フルヴィッツ数のほかにも，モジュラー方程式を応用した虚 2 次体のフルヴィッツの類数関係式，リーマン面のフルヴィッツ公式や自己同型群の研究，四元数環その他の代数の研究など，彼の名前を目にする分野は多岐にわたる．また Hilbert によれ

---

[7]Hermann Cäsar Hannibal Schubert（1848.5.22 ドイツ Potsdam 生――1911.7.20 ドイツ Hamburg 没）

[8]Felix Christian Klein（1849.4.25 ドイツ Düsseldorf 生――1925.6.22 ドイツ Göttingen 没）

[9]Carl Louis Ferdinand von Lindemann（1852.4.12 ドイツ Hannover 生――1939.3.6 ドイツ München 没）．1882 年，円周率 π が超越数であることを証明．

[10]David Hilbert（1862.1.23 プロイセン Königsberg（現ロシア Kaliningrad）生――1943.2.14 ドイツ Göttingen 没）

[11]Hermann Minkowski（1864.6.22 ロシア Alexotas（現リトアニア Kaunas）生――1909.1.12 ドイツ Göttingen 没）

[12]Ferdinand Georg Frobenius（1849.10.26 ドイツ Berlin-Charlottenburg 生――1917.8.3 ドイツ Berlin 没）

ば，Hurwitz の特に好んだテーマが連分数であったという（5 編ばかり論文を書いている）．

非常に控え目な，礼儀正しい人であったらしい．彼の全集を主として編纂した Pólya[13]によれば，近所の使用人にも帽子をとって挨拶をする人であったという [69]．また，若いころは数学者になるかピアニストになるかと迷ったというほどのピアノの名手でもあった．1919 年 11 月 18 日，60 才でこの世を去った．

[13]George Pólya（1887.12.13 ハンガリー Budapest 生——1985.9.7 アメリカ Palo Alto 没）

第 13 章

バーンズの多重ゼータ関数

この章では，フルヴィッツゼータ関数の自然な拡張であるバーンズの多重ゼータ関数を導入し，その解析接続を与え，負整数点での特殊値をベルヌーイ多項式を用いて記述する．さらに，2 重ゼータ関数については関数等式を求めることを問題にする．このとき，関数等式にある種のレルヒ[1]型ゼータ関数が現れることや，証明に保型形式的手法を用いることなど，興味深い点も多い．

バーンズの多重ゼータ関数を説明する動機は，これが実 2 次体（総実代数体）の類体構成問題に関する重要で興味深い予想（Stark・新谷[2]の予想，[76], [77] など参照）と深く関係するからである．この本では扱わないが，バーンズの多重ゼータ関数の 1 階微分の $s=0$ での値は多重ガンマ関数と呼ばれる特殊関数の特殊値で表される．新谷氏は，実 2 次体の類体構成には 2 重ガンマ関数の特殊値が重要な役割を担うことを看破し，2 重ガンマ関数の適当な特殊値が実際に類体を構成するであろうという精密な予想を提出，その一部分を解決した（[75], [76], [77]）．虚 2 次体の類体構成の場合には，j-不変量などの保型関数がきわめて重要な役割を果たすが，実 2 次体の場合，[76] には保型関数的視点はなかった．この章で扱うレルヒ型ゼータ関数は，実 2 次体の類体構成問題に，多少なりともそのような観点を付与する試みを意図して導入されたものである．詳しくは [4], [5] を参照されたい．

---

[1] Mathias Lerch（1860.2.20 チェコ Milinov 生――1922.8.3 チェコ Susice 没）

[2] 新谷卓郎（1943.2.4 北九州生――1980.11.14 東京没）

13.1　多重ゼータ関数の特殊値とベルヌーイ多項式

$a, w_1, w_2, \cdots, w_r$ はすべて正の実数とする．$\mathbf{w} = (w_1, \cdots, w_r)$ とおき，ゼータ関数 $\zeta(s, \mathbf{w}, a)$ を

$$\zeta(s, \mathbf{w}, a) = \sum_{m_1=0}^{\infty} \cdots \sum_{m_r=0}^{\infty} (a + m_1 w_1 + \cdots + m_r w_r)^{-s}$$

で定義する．このゼータ関数は $\mathrm{Re}(s) > r$ で絶対収束する．この種のゼータ関数は Barnes[3]によって組織的に研究された（[9], [10]）．

しばらく $\mathrm{Re}(s) > r$ とする．$\zeta(s, \mathbf{w}, a)$ は

$$\begin{aligned}
\zeta(s, \mathbf{w}, a) &= \frac{1}{\Gamma(s)} \sum_{m_1=0}^{\infty} \cdots \sum_{m_r=0}^{\infty} \int_0^{\infty} t^{s-1} e^{-(a+m_1 w_1+\cdots+m_r w_r)t}\, dt \\
&= \frac{1}{\Gamma(s)} \int_0^{\infty} t^{s-1} \sum_{m_1=0}^{\infty} \cdots \sum_{m_r=0}^{\infty} e^{-(a+m_1 w_1+\cdots+m_r w_r)t}\, dt \\
&= \frac{1}{\Gamma(s)} \int_0^{\infty} t^{s-1} \frac{e^{-at}}{(1-e^{-w_1 t})\cdots(1-e^{-w_r t})}\, dt \\
&= \frac{1}{\Gamma(s)} \int_0^{\infty} t^{s-1} \frac{e^{(w_1+\cdots+w_r-a)t}}{(e^{w_1 t}-1)\cdots(e^{w_r t}-1)}\, dt
\end{aligned}$$

と変形される．級数 $\zeta(s, \mathbf{w}, a)$ は $\mathrm{Re}(s) > r$ で絶対収束するので，ルベーグ[4]積分の有界収束定理などを使えば，同じ s の範囲でこの変形は正当化される．$r = 1$ のときは，本質的にフルヴィッツゼータ関数である．すなわち $w_1 > 0$ に対して

$$\zeta(s, w_1, a) = w_1^{-s} \zeta\left(s, \frac{a}{w_1}\right)$$

となる．さて多重ゼータ関数 $\zeta(s, \mathbf{w}, a)$ についても，フルビッツゼータ関数のときと同様に，これをコンタワー積分の形に表示できる．実際，$\varepsilon > 0$ を十分小さくとり，$I(\varepsilon, \infty)$ を 9.2 節の積分路として

---

[3]Ernest Barnes（1874.4.1 イギリス Birmingham 生——1953.11.29 イギリス Sussex 没）

[4]Henri Léon Lebesgue（1875.6.28 フランス Beauvais(Oise) 生——1941.7.26 フランス Paris 没）

$$\zeta(s,\mathbf{w},a)=\frac{1}{\Gamma(s)(e^{2\pi is}-1)}\int_{I(\varepsilon,\infty)}t^{s-1}\frac{e^{(w_1+\cdots+w_r-a)t}}{(e^{w_1t}-1)\cdots(e^{w_rt}-1)}\,dt \qquad (13.1)$$

となる．この表示の優れている点は，これによって $\zeta(s,\mathbf{w},a)$ が全 s 平面の有理型関数に解析接続されることにある．なぜなら，右辺のコンタワー積分は，任意の $s\in\mathbf{C}$ に対して絶対収束し，s の全平面での正則関数を表すからである．

$\zeta(s,\mathbf{w},a)$ の極になりうる点は，絶対収束領域にない $e^{2\pi is}-1$ の零点

$$s=r,\ r-1,\ \cdots,\ 0,\ -1,\ -2,\ \cdots$$

であるが，$\Gamma(s)$ が 0 以下の整数点に 1 位の極をもつことから点 $s=1-m$ $(m\in\mathbf{N})$ では極は現れず，$\zeta(s,\mathbf{w},a)$ はここで正則になる．

$\zeta(s,\mathbf{w},a)$ の整数点 $s=1-m$ $(m\in\mathbf{N})$ での特殊値を求めてみよう．フルヴィッツゼータ関数の特殊値を求めたのと同じ手法による．

命題 13.1　$m\in\mathbf{N}$ とする．$a>0$ に対して

$$a=a_1w_1+a_2w_2+\cdots+a_rw_r \qquad (a_1,a_2,\cdots,a_r\in\mathbf{R})$$

と表すとき

$$\zeta(1-m,\mathbf{w},a)=$$
$$(-1)^r(m-1)!\sum_{\substack{m_1+\cdots+m_r=m+r-1\\ m_1\geq 0,\cdots,m_r\geq 0}}\left(\prod_{j=1}^{r}\frac{B_{m_j}(a_j)}{m_j!}\right)w_1^{m_1-1}\cdots w_r^{m_r-1}$$

となる．ただし，和において $m_1,m_2,\cdots,m_r$ は条件 $m_1+\cdots+m_r=m+r-1$, $m_1\geq 0,\cdots,m_r\geq 0$ を満たすすべての整数を動く．

証明　命題 9.3 の証明と同様にして

$$\zeta(1-m,\mathbf{w},a)=\left(\lim_{s\to 1-m}\frac{1}{\Gamma(s)(e^{2\pi is}-1)}\right)\int_{I(\varepsilon)}t^{-m}\frac{e^{(w_1+\cdots+w_r-a)t}}{(e^{w_1t}-1)\cdots(e^{w_rt}-1)}\,dt$$
$$=\frac{(-1)^{m-1}(m-1)!}{2\pi i}\int_{I(\varepsilon)}t^{-m}\prod_{j=1}^{r}\frac{e^{(1-a_j)w_jt}}{e^{w_jt}-1}\,dt$$

となる．ここで，被積分関数のローラン展開は，ベルヌーイ多項式の母関数（56 ページ (4.2) 式）と命題 4.9 の (4) を用いることにより

$$t^{-m}\prod_{j=1}^{r}\frac{e^{(1-a_j)w_jt}}{e^{w_jt}-1}=t^{-m}\sum_{m_1=0}^{\infty}\cdots\sum_{m_r=0}^{\infty}\prod_{j=1}^{r}\left(B_{m_j}(1-a_j)\frac{(w_jt)^{m_j-1}}{m_j!}\right)$$

$$=\sum_{m_1=0}^{\infty}\cdots\sum_{m_r=0}^{\infty}\left(\prod_{j=1}^{r}\frac{(-1)^{m_j}B_{m_j}(a_j)w_j^{m_j-1}}{m_j!}\right)t^{m_1+\cdots+m_r-r-m}$$

である．この被積分関数の $t=0$ での留数は

$$\sum_{\substack{m_1+\cdots+m_r=m+r-1\\ m_1\geq 0,\cdots,m_r\geq 0}}\left(\prod_{j=1}^{r}(-1)^{m_j}\frac{B_{m_j}(a_j)w_j^{m_j-1}}{m_j!}\right)$$

となるから，命題の結果を得る．∎

13.2　2重ゼータ関数とある種のディリクレ級数

いま，$\mathbf{w}=(w_1,w_2)$ とする．バーンズの2重ゼータ関数 $\zeta(s,\mathbf{w},a)$ のコンタワー積分表示 (13.1) において，フルヴィッツゼータ関数の関数等式（定理 9.4）を求めたのと同じ手法で，コンタワー積分を切り開くと，どんなゼータ関数が出現するかを考察することは大変興味深い問題であろう．

いま，代数的実無理数[5] α に対して次のディリクレ級数

$$\xi(s,\alpha)=\sum_{n=1}^{\infty}\frac{\cot\pi n\alpha}{n^s}$$

を考えよう．まず $\mathrm{Re}(s)$ が十分大のとき収束することを示す必要がある．

超越数論のディオファンタス近似に関するロス (Roth) の定理により，次のことが知られている．α は代数的実無理数とする．任意の正数 ε をとるとき，ある正定数 $C(\varepsilon)$ が存在して，任意の整数 m, n $(n>0)$ に対して

$$\left|\alpha-\frac{m}{n}\right|>C(\varepsilon)n^{-2-\varepsilon} \tag{13.2}$$

となる．いま，実数 x に対し $\langle\langle x\rangle\rangle$ を x と最も近くにある整数との距離を表すとする．$0\leq\langle\langle x\rangle\rangle\leq 1/2$ である．この記号を用いると，(13.2) 式は任意の正整

[5] 有理数でない実の代数的数．

数 n に対し

$$\langle\langle n\alpha\rangle\rangle > C(\varepsilon)n^{-1-\varepsilon}$$

と表現できる．$0<x<\pi/2$ のとき $\sin x > \frac{2}{\pi}x$ が成り立つので

$$|\cot\pi n\alpha| \le \frac{1}{\sin\pi\langle\langle n\alpha\rangle\rangle} < \frac{1}{2\langle\langle n\alpha\rangle\rangle}$$

$$< \frac{1}{2C(\varepsilon)}n^{1+\varepsilon}.$$

この評価から，$\sigma=\mathrm{Re}(s)$ とおくと，$\xi(s,\alpha)$ の優級数として

$$\frac{1}{2C(\varepsilon)}\sum_{n=1}^{\infty}\frac{n^{1+\varepsilon}}{n^{\sigma}}$$

がとれ，$\sigma>2+\varepsilon$ で収束する．ε は任意にとってよいので $\xi(s,\alpha)$ は $\mathrm{Re}(s)>2$ で収束し[6]，しかも広義一様収束するので，その範囲で s の正則関数になる．

$SL_2(\mathbf{Z})$ を前出（76ページ）のモジュラー群とする．$SL_2(\mathbf{Z})$ の元 $V=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ を代数的実無理数 α に

$$V\alpha = \frac{a\alpha+b}{c\alpha+d}$$

で作用させると $V\alpha$ も代数的実無理数になる．以下で保型因子の記号

$$J(V,\alpha)=c\alpha+d \tag{13.3}$$

を用いる．

ω と a を正数とし，2 重ゼータ関数

$$\zeta_2(s,\omega,a)=\sum_{m,\,n=0}^{\infty}(m+n\omega+a)^{-s}$$

を考えよう．以前の記号では $\zeta_2(s,\omega,a)=\zeta(s,(1,\omega),a)$ である．

$$\gamma(s)=\frac{(2\pi)^s}{\Gamma(s)\sin(\pi s/2)}$$

とおく．$\zeta_2(s,\omega,a)$ は $\mathrm{Re}(s)>2$ で絶対収束し，そこで正則で，全 s 平面の有理型関数に解析接続され，極は $s=1,\ 2$ で 1 位である．$s=1$ でのローラン展開の主要部は，コンタワー積分表示 (13.1) より，

[6] 実はロスの定理をもう少し有効に使うと $\mathrm{Re}(s)>1$ で絶対収束することが示せる（[4] 参照）．

$$\zeta_2(s,\omega,a)=\left(\frac{1+\omega}{2\omega}-\frac{a}{\omega}\right)\frac{1}{s-1}+\cdots \tag{13.4}$$

で与えられる．

命題 13.2　$\alpha>0$ を代数的実無理数とする．$V=\begin{pmatrix} n & -1 \\ 1 & 0 \end{pmatrix}$　$(n\in\mathbf{Z})$ とすると，$\mathrm{Re}(s)>2$ の範囲で

$$\alpha^{s-1}\xi(s,V\alpha)-\xi(s,\alpha)=(1-\alpha^{s-1})\cot(\pi s/2)\zeta(s)-\gamma(s)\zeta_2(1-s,\alpha,1) \tag{13.5}$$

なる変換式が成立する．

証明　2 重ゼータ関数 $\zeta_2(s,\alpha,1)$ のコンタワー積分表示

$$\zeta_2(s,\alpha,1)=\frac{1}{\Gamma(s)(e^{2\pi is}-1)}\int_{I(\varepsilon,\infty)}t^{s-1}\frac{e^{\alpha t}}{(e^t-1)(e^{\alpha t}-1)}\,dt \tag{13.6}$$

から出発する．この式は (13.1) 式で $r=2$, $w_1=1$, $w_2=\alpha$, $a=1$ とすればよい．右辺は s の全平面の有理型関数に解析接続されているので，$\mathrm{Re}(s)<-1$ の範囲で考えよう．$t_0<0$ とし，$C(t_0)$ を $\mathrm{Re}(t)=t_0$ で表される上向きの直線とする．すなわち

$$C(t_0): t=t_0+iy \qquad (-\infty<y<\infty).$$

定理 9.4 の証明と同様に積分路 $I(\varepsilon,\infty)$ を $C(t_0)$ まで左にシフトして留数定理を使うことにより

$$\zeta_2(s,\alpha,1)=\frac{1}{\Gamma(s)(e^{2\pi is}-1)}\left\{-\int_{C(t_0)}t^{s-1}\frac{e^{\alpha t}}{(e^t-1)(e^{\alpha t}-1)}\,dt\right.$$
$$\left.-2\pi i\sum_{n\in\mathbf{Z}-\{0\}}\left(\frac{(2\pi in)^{s-1}}{1-e^{-2\pi in\alpha}}+\frac{(2\pi in/\alpha)^{s-1}}{e^{2\pi in/\alpha}-1}\cdot\frac{1}{\alpha}\right)\right\}$$

と変形され，さらに $t_0\to-\infty$ とし，

$$\frac{1}{1-e^{-2\pi in\alpha}}=\frac{1}{2i}\cot\pi n\alpha+\frac{1}{2}\quad \text{および}\quad \frac{1}{e^{2\pi in/\alpha}-1}=\frac{1}{2i}\cot\frac{\pi n}{\alpha}-\frac{1}{2}$$

に注意すると，

$$\zeta_2(s,\alpha,1)=\frac{-2\pi i(2\pi)^{s-1}}{\Gamma(s)(e^{2\pi is}-1)}\left\{-\frac{e^{\pi is/2}(1+e^{\pi is})}{2}\left(\xi(1-s,\alpha)+\alpha^{-s}\xi\left(1-s,\frac{1}{\alpha}\right)\right)+\frac{e^{\pi is/2}(1-e^{\pi is})}{2i}(1-\alpha^{-s})\zeta(1-s)\right\}$$

まで変形される．ここまでの変形は $\mathrm{Re}(s)<-1$ で成り立つ．s に $1-s$ を代入し，$\Gamma(s)\Gamma(1-s)=\pi/\sin\pi s$ を使うと，$\mathrm{Re}(s)>2$ の範囲で

$$\begin{aligned}&\zeta_2(1-s,\alpha,1)\\&=(2\pi)^{-s}\Gamma(s)\sin\pi s\left\{\frac{e^{-\pi is/2}(1-e^{-\pi is})}{1-e^{-2\pi is}}\left(\xi(s,\alpha)+\alpha^{s-1}\xi\left(s,\frac{1}{\alpha}\right)\right)\right.\\&\qquad\left.+\frac{ie^{-\pi is/2}(1+e^{-\pi is})}{1-e^{-2\pi is}}(1-\alpha^{s-1})\zeta(s)\right\}\\&=\frac{1}{\gamma(s)}\left\{\xi(s,\alpha)-\alpha^{s-1}\xi\left(s,-\frac{1}{\alpha}\right)+(1-\alpha^{s-1})\cot(\pi s/2)\zeta(s)\right\}\end{aligned}$$

となり，整理すると

$$\alpha^{s-1}\xi\left(s,-\frac{1}{\alpha}\right)-\xi(s,\alpha)=(1-\alpha^{s-1})\cot(\pi s/2)\zeta(s)-\gamma(s)\zeta_2(1-s,\alpha,1).$$

ゆえに $\xi(\alpha+n,s)=\xi(\alpha,s)$ に注意すれば定理の主張を得る．∎

この変換式 (13.5) は次の形に拡張されている．$x\in\mathbf{R}$ について $\{x\}$ は $x-\{x\}\in\mathbf{Z}$, $0\leq\{x\}<1$ を満たす実数（x の小数部分）とする．

定理 13.3　代数的実無理数 α と $V=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in SL_2(\mathbf{Z})$ が $c>0$, $c\alpha+d>0$ を満たすとき，$\mathrm{Re}(s)>2$ の範囲で，変換公式

$$\eta^{s-1}\xi(s,V\alpha)-\xi(s,\alpha)=(1-\eta^{s-1})\cot(\frac{\pi s}{2})\zeta(s)-\gamma(s)\sum_{j\bmod c}\zeta_2(1-s,\eta,x_j+y_j\eta)$$

が成り立つ．ただし，$\eta=c\alpha+d$ とおき，j は c を法とする剰余類を代表する整数を動く．各 $j\bmod c$ について $x_j=1-\{jd/c\}$, $y_j=\{j/c\}$ とおいた．

この定理で $V=\begin{pmatrix}n & -1\\ 1 & 0\end{pmatrix}$ とすれば命題 13.2 の変換式になる．定理の証明に興味のある方は [4], [5] を参照されたい．

ここから α は実 2 次無理数とする．このとき，$V = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})$ で，条件

$$V\alpha = \alpha, \quad c\alpha + d > 0 \tag{13.7}$$

を満たすものが存在する．このことは次のように考えると見やすい．F を実 2 次体 $\mathbf{Q}(\alpha)$ とする．$L = \mathbf{Z}\alpha + \mathbf{Z}$ を α と 1 で生成される格子とし，$\mathcal{O}(L)$ を L の整環（order）とする．すなわち，$\mathcal{O}(L) = \{u \in F \mid uL \subset L\}$．$\mathcal{O}(L)$ の総正単数群を $E(L)$ と記す．$E(L)$ の元 η で $\eta \neq 1$ なるものをとる．$\eta \in L, \eta\alpha \in L$ であるので $\mathbf{Z}$ 係数の 2 次行列 V を

$$\eta \begin{pmatrix} \alpha \\ 1 \end{pmatrix} = V \begin{pmatrix} \alpha \\ 1 \end{pmatrix}, \qquad V = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

で定めると $V \in SL_2(\mathbf{Z})$ であり，$\eta = c\alpha + d > 0$ となる．$c > 0$ にするには，$\alpha > \alpha'$（α' は α の共役）ならば $\eta > 1$ なる η をとり，$\alpha < \alpha'$ ならば $0 < \eta < 1$ なる η をとればよい．

定理 13.3 をこの状況に適用して次の定理を得る．

定理 13.4　実 2 次無理数 α が与えられたとき，F の総正単数 η で

$$\eta \begin{pmatrix} \alpha \\ 1 \end{pmatrix} = V \begin{pmatrix} \alpha \\ 1 \end{pmatrix}, \qquad V = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})$$

かつ $c > 0$ を満たすものをとる．このとき，$\mathrm{Re}(s) > 2$ の範囲で，

$$\xi(s, \alpha) = -\cot(\pi s/2)\zeta(s) + \frac{\gamma(s)}{1 - \eta^{s-1}} \sum_{j \bmod c} \zeta_2(1 - s, \eta, x_j + y_j\eta) \tag{13.8}$$

となる．この式により $\xi(s, \alpha)$ は全 s 平面の有理型関数に解析接続され，極は $s = 1$ および $s = 1 + \frac{2\pi i n}{\log \eta}$ ($n \in \mathbf{Z}$, $n \neq 0$) で 1 位である．さらに $s = 2m - 1$ ($m \in \mathbf{Z}$, $m \geq 2$) での特殊値がベルヌーイ多項式を用いて

$$\xi(2m - 1, \alpha) = \frac{(-1)^{m-1}(2\pi)^{2m-1}}{1 - \eta^{2m-2}} \sum_{k=0}^{2m} \sum_{j \bmod c} \frac{B_k(x_j)B_{2m-k}(y_j)}{k!(2m - k)!} \eta^{2m-k-1}$$

と表現される[7].

証明 (13.8) 式は定理 13.3 で $V\alpha=\alpha$ を用いれば直ちに導かれる．極をとる可能性があるのは，$s=2$, $s=1$, $s=1+\frac{2\pi in}{\log\eta}$ $(n\in\mathbf{Z},\ n\neq 0)$，および $s=0$ である．$s=-2,\ -4,\ -6,\cdots$ では，$\zeta(s)=0$ であるので，極にはならないことに注意する．$s=2$ については，205 ページの脚注で注意したように，$\xi(s,\alpha)$ は $\mathrm{Re}(s)>1$ で絶対収束し，そこで正則になるので，極にはなり得ない．$s=0$ を考えよう．$\zeta_2(s,\omega,a)$ の $s=1$ での極の主要部が (13.4) 式で与えられることと $\zeta(0)=-\frac{1}{2}$ を考慮に入れると，関数 $\xi(s,\alpha)$ の $s=0$（高々1 位の極）での留数は

$$\frac{1}{\pi}-\frac{2}{\pi(1-\eta^{-1})}\sum_{j \bmod c}\left(\frac{1+\eta}{2\eta}-\frac{x_j+y_j\eta}{\eta}\right)$$

で与えられる．この値は容易に零になることがわかるので，$\xi(s,\alpha)$ は $s=0$ で正則になる．

最後に $s=2m-1$ $(m\in\mathbf{Z},\ m\geq 2)$ での特殊値は (13.8) 式により，

$$\xi(2m-1,\alpha)=\frac{(-1)^{m-1}(2\pi)^{2m-1}}{(1-\eta^{2m-2})(2m-2)!}\sum_{j \bmod c}\zeta_2(2-2m,\eta,x_j+y_j\eta)$$

となり，命題 13.1 により，ベルヌーイ多項式を用いた表示が得られる．∎

13.3 $\xi(s,\alpha)$ と連分数

D. Zagier 著の『数論入門』([94, §13]) に詳しく記述されているように，任意の実 2 次無理数 β は次の形の連分数に展開される[8].

$$\beta=b_1-\cfrac{1}{b_2-\cfrac{1}{b_3-\cfrac{1}{b_4-\ddots}}}\qquad (b_j\in\mathbf{Z},\ b_2,b_3,\cdots\geq 2).$$

2 番目以降の係数 b_j $(j\geq 2)$ が 2 以上の整数になるところが重要である．ここで，数列 $\{b_1,b_2,\cdots\}$ は周期的，すなわち，ある自然数 ν と r があって，ν から先の j については

---

[7] この種の特殊値は，α が実 2 次体の単数のときに Berndt [12] によって計算されている．

[8] ここで扱う連分数は通常の実 2 次無理数の連分数展開とは異なる．

$$b_{r+j} = b_j \qquad (j \geq \nu)$$

となる．このような最小の自然数 r を β の周期と呼ぶ．この連分数展開を

$$\beta = [[b_1, b_2, \cdots, b_{\nu-1}, \overline{b_\nu, \cdots, b_{\nu+r-1}}\,]] \tag{13.9}$$

と表すことにしよう．$\{b_\nu, \cdots, b_{\nu+r-1}\}$ は基本周期と呼ばれる．また，$\nu = 1$ のとき，すなわち最初から周期的となるとき，β の連分数展開は純周期的であるという．

実 2 次無理数 β の共役数を β' で表す．いま，実 2 次無理数 ω の連分数展開が純周期的とし，連分数展開を

$$\omega = [[\,\overline{n_1, n_2, \cdots, n_r}\,]] \qquad (n_j \geq 2)$$

とする．このとき，

$$\frac{1}{\omega'} = [[\,\overline{n_r, n_{r-1}, \cdots, n_1}\,]]$$

となる（[94, p.136, (17)]）．この表示より，

$$\omega > 1 \quad \text{かつ} \quad 0 < \omega' < 1 \tag{13.10}$$

となる．実 2 次無理数 ω がこの条件(13.10) を満たすとき，ω は簡約的[9]と呼ばれる．

逆に ω がこの条件を満たせば ω の連分数展開は純周期的であることが示せるので，ω が簡約的であることは ω の連分数展開が純周期的であるための必要十分条件である．

F を実 2 次体とし，F は実数体 $\mathbf{R}$ に埋め込まれているとする．さらに，F から $\mathbf{R} \times \mathbf{R}$ への対応を

$$F \ni \theta \longmapsto (\theta, \theta') \in \mathbf{R} \times \mathbf{R}$$

で定め，θ を $\mathbf{R} \times \mathbf{R}$ の点 (θ, θ') と同一視する．いま，$\omega \in F - \mathbf{Q}$ は簡約的とし，ω の連分数展開を

$$\omega = [[\,\overline{n_1, n_2, \cdots, n_r}\,]]$$

とする．整数列 $\{n_j\}_{j \in \mathbf{Z}}$ を連分数展開の $\{n_1, n_2, \cdots, n_r\}$ を延長して周期性により，任意の $j \in \mathbf{Z}$ に対し $n_{j+r} = n_j$ となるように定義する．正整数 i に対し

$$\omega_i = [[\,\overline{n_i, n_{i+1}, \cdots, n_{i+r-1}}\,]] \tag{13.11}$$

[9]通常の簡約的と異なる．通常，実 2 次無理数 α が簡約的とは $\alpha > 1$ かつ $0 > \alpha' > -1$ のときをいう．

で簡約的な数 ω_i を定義する．もちろん $\omega_1 = \omega_{r+1} = \omega$ である．$n \in \mathbf{Z}$ に対し

$$V(n) = \begin{pmatrix} n & -1 \\ 1 & 0 \end{pmatrix} \in SL_2(\mathbf{Z})$$

とおく．連分数展開 (13.11) の形から

$$\omega_i = n_i - \frac{1}{\omega_{i+1}} = V(n_i)\omega_{i+1}$$

となるので，

$$\omega = V(n_1)V(n_2)\cdots V(n_r)\omega$$

が成り立つ．いま，F の格子 L を

$$L = \mathbf{Z}\omega + \mathbf{Z}$$

で定義し，$\mathcal{O}(L)$ の総正単数群 $E(L)$ の基本単数 ε を $\varepsilon > 1$ にとる．

$$\varepsilon \begin{pmatrix} \omega \\ 1 \end{pmatrix} = V \begin{pmatrix} \omega \\ 1 \end{pmatrix}, \qquad V = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})$$

の関係で V を定める．双曲点 ω の固定部分群 $\Gamma_\omega = \{M \in SL_2(\mathbf{Z}) \mid M\omega = \omega\}$ を考えると，Γ_ω は V と $\pm I_2$（I_2 は単位行列）で生成される．$c > 0$ だから r が ω の周期であることにより，

$$V = V(n_1)V(n_2)\cdots V(n_r)$$

が成り立つ．このとき保型因子 (13.3) の性質を使って

$$\begin{aligned}\varepsilon = J(V,\omega) &= J(V(n_1),\omega_2)J(V(n_2),\omega_3)\cdots J(V(n_r),\omega) \\ &= \omega_2\omega_3\cdots\omega_r\omega.\end{aligned}$$

これより，

$$\varepsilon = \omega_1\omega_2\cdots\omega_r \tag{13.12}$$

が従う．そこで，$\xi_0 = 1, \xi_1 = \omega = \omega_{r+1}, \xi_2 = \omega_{r+1}\omega_r, \cdots, \xi_r = \omega_{r+1}\omega_r\cdots\omega_2$ とおく．もちろん，$\xi_r = \varepsilon$ である．ここで

$$L = \mathbf{Z}\xi_i + \mathbf{Z}\xi_{i+1} \qquad (0 \le i \le r-1) \tag{13.13}$$

である．なぜなら，$\xi_{i-1} = \xi_i \cdot \frac{1}{\omega_{r+2-i}}$ より

$$\mathbf{Z}\xi_{i-1}+\mathbf{Z}\xi_i=\xi_i\big(\mathbf{Z}\frac{1}{\omega_{r+2-i}}+\mathbf{Z}\big)$$

$$=\xi_i\Big(\mathbf{Z}(n_{r+1-i}-\omega_{r+1-i})+\mathbf{Z}\Big)$$

$$=\mathbf{Z}\xi_i+\mathbf{Z}\xi_{i+1}$$

となり，$i=1$ から始めれば示せる．さて格子 L の 2 重ゼータ関数を

$$\Xi_L(s)=\sum_{\theta\in L\bigcap C(1,\varepsilon)}\theta^{-s} \tag{13.14}$$

で定義する．ここで $C(1,\varepsilon)$ は

$$C(1,\varepsilon)=\{(x+y\varepsilon,x+y\varepsilon')\mid x>0,\ y\geq 0\}$$

で与えられる錐体（simplicial cone）である．後で見るように $\Xi_L(s)$ はいままでの 2 重ゼータ関数の有限和の形に書けるので，$\mathrm{Re}(s)>2$ で絶対収束し，その範囲で正則である．

$\mathbf{R}_+$ は正数のなす集合とする．総正単数群 $E(L)$ は

$$\eta(u,v)=(\eta u,\eta' v)\qquad (\eta\in E(L),\ (u,v)\in\mathbf{R}_+\times\mathbf{R}_+)$$

により，$\mathbf{R}_+\times\mathbf{R}_+$ に作用する．$C(1,\varepsilon)$ はこの作用に関する $\mathbf{R}_+\times\mathbf{R}_+$ の $E(L)$ による基本領域である．各 $\omega_i>1$ だから

$$C(1,\varepsilon)=\bigcup_{k=1}^{r}\{x\xi_{k-1}+y\xi_k\mid x>0,\ y\geq 0\}\quad(\text{直和})$$

と表されるので，(13.13) 式より

$$L\cap C(1,\varepsilon)=\bigcup_{k=1}^{r}\{m\xi_{k-1}+n\xi_k\mid m\in\mathbf{Z}_{>0},\ n\in\mathbf{Z}_{\geq 0}\}\quad(\text{直和}) \tag{13.15}$$

である．この分解は Zagier [92] で与えられた．ここで，$\mathbf{Z}_{>0}$ ($\mathbf{Z}_{\geq 0}$) は正の整数の集合（0 以上の整数の集合）を表す．分解 (13.15) により，

$$\Xi_L(s)=\sum_{k=1}^{r}(\xi_{k-1})^{-s}\zeta_2(s,\omega_{r+2-k},1) \tag{13.16}$$

を得る．この表示式により，$\Xi_L(s)$ は $\mathrm{Re}(s)>2$ で絶対収束し，全 s 平面の $s=1,\ 2$ 以外で正則な有理型関数に解析接続される．

関数 $\xi(s,\omega)$ と $\Xi_L(s)$ の間には次の関数等式が成り立つ．

定理 13.5　ω は F の簡約的な数，$L=\mathbf{Z}+\mathbf{Z}\omega$ とし，$\varepsilon>1$ は L の整環 $\mathcal{O}(L)$

の総正基本単数とする．このとき

$$\xi(s,\omega) = -\cot(\pi s/2)\zeta(s) - \frac{\gamma(s)}{\varepsilon^{s-1}-1}\Xi_L(1-s) \tag{13.17}$$

が成り立つ．この等式を通じても $\xi(s,\omega)$ は s の有理型関数に解析接続される．

証明 いま，$\omega_i = V(n_i)\omega_{i+1}$ かつ $\omega_i > 0$ であるから，命題 13.2 により，等式

$$(\omega_{r+2-k})^{s-1}\xi(s,\omega_{r+1-k}) - \xi(s,\omega_{r+2-k})$$

$$= \left(1-(\omega_{r+2-k})^{s-1}\right)\cot(\pi s/2)\zeta(s) - \gamma(s)\zeta_2(1-s,\omega_{r+2-k},1)$$

が $1 \le k \le r$ で成り立つ．この等式の両辺に $(\xi_{k-1})^{s-1}$ をかけて $k=1$ から $k=r$ まで足しあわせて，(13.12) 式と (13.16) 式を用いると

$$(\varepsilon^{s-1}-1)\xi(s,\omega) = (1-\varepsilon^{s-1})\cot(\pi s/2)\zeta(s) - \gamma(s)\Xi_L(1-s)$$

を得る． ∎

注意 13.6 2 重ゼータ関数のみでなく多重ゼータ関数のコンタワー積分表示を 13.2 節と同様の方法で切り開くと，やはりある種のレルヒ型ゼータ関数が現れるが，それがどのような保型的（モジュラー）な性質をもつかを調べることは興味深い問題であろう．

第 14 章

多重ベルヌーイ数

第 4 章で一般ベルヌーイ数を定義したが，この章ではベルヌーイ数のまた別の一般化の 1 つである，多重ベルヌーイ数 (poly-Bernoulli numbers) というものを定義し，そのいくつかの性質を調べる．

14.1　多重ベルヌーイ数

まずは天下りに次のように定義をする．

定義 14.1（多重ベルヌーイ数） 多重ベルヌーイ数 $\mathbb{B}_n^{(k)} \in \mathbf{Q}$ $(n \geq 0,\ k \in \mathbf{Z})$ を，母関数により

$$\frac{Li_k(1-e^{-t})}{1-e^{-t}} = \sum_{n=0}^{\infty} \mathbb{B}_n^{(k)} \frac{t^n}{n!}$$

で定義する．ここに整数 k に対し $Li_k(t)$ は形式的べき級数 $\displaystyle\sum_{n=1}^{\infty} \frac{t^n}{n^k}$ を表す．

この $Li_k(t)$ は，$k \geq 1$ ならいわゆる多重対数関数（polylogarithm，これが $\mathbb{B}_n^{(k)}$ の名前の由来）で，$k \leq 0$ のときは有理関数 $\left(t\frac{d}{dt}\right)^{-k}\left(\frac{t}{1-t}\right)$ の原点におけるテイラー展開級数である．$k=1$ のとき $Li_1(t) = -\log(1-t)$ で，$Li_1(1-e^{-t}) = t$ であるから，19 ページ定理 1.12 より，$\mathbb{B}_n^{(1)}$ はベルヌーイ数 B_n にほかならない．$k \geq 1$ のときは $Li_k(t)$ の「反復積分」表示

$$Li_k(t) = \int_0^t \frac{dt_k}{t_k} \int_0^{t_k} \frac{dt_{k-1}}{t_{k-1}} \cdots \int_0^{t_3} \frac{dt_2}{t_2} \int_0^{t_2} \frac{dt_1}{1-t_1}$$

において，変数変換 $t_i \mapsto 1 - e^{-t_i}$ を行うことにより，

$$\begin{aligned}&\frac{Li_k(1-e^{-t})}{1-e^{-t}}\\&= e^t \cdot \frac{1}{e^t-1}\int_0^t \frac{dt_k}{e^{t_k}-1}\int_0^{t_k}\frac{dt_{k-1}}{e^{t_{k-1}}-1}\int_0^{t_{k-1}}\cdots\int_0^{t_3}\frac{dt_2}{e^{t_2}-1}\int_0^{t_2}dt_1\end{aligned} \tag{14.1}$$

とも書かれる．すなわち，$k \geq 1$ の場合の多重ベルヌーイ数 $\mathbb{B}_n^{(k)}$ の母関数 $\sum_{n=0}^{\infty}\mathbb{B}_n^{(k)}\frac{t^n}{n!}$ は，1 から出発し，積分 $\int_0^t dt$ を行い e^t-1 で割る，という操作を k 回繰り返し，最後に e^t をかけることによって得られる．

注意 14.2

(1)　多重ベルヌーイ数は「高次ベルヌーイ数」(Bernoulli numbers of higher order, [68]) とは異なる．高次ベルヌーイ数の母関数は $\left(\frac{t}{e^t-1}\right)^k$ である．これは本質的に $\frac{t}{e^t-1}$ の微分の適当な線形結合として書けるので，高次ベルヌーイ数は古典的ベルヌーイ数の線形結合で書ける．それに対し $\mathbb{B}_n^{(k)}$ は，後の漸化式が示すようにやはり古典的ベルヌーイ数で書けるが，積を次々にとっていかなければならない．

(2)　リーマンゼータ関数の正整数点での値を一般化した多重ゼータ値というものがあり，それはこの多重ベルヌーイ数と無関係ではない（[7]，[96] などを参照）．

ここで $k \geq 0$ のときの $\mathbb{B}_n^{(k)}$ について，いくつかの値を表にしておく．

表 14.1: $\mathbb{B}_n^{(k)}$ $(0 \leq k \leq 5,\ 0 \leq n \leq 7)$

k \ n	0	1	2	3	4	5	6	7
0	1	1	1	1	1	1	1	1
1	1	$\frac{1}{2}$	$\frac{1}{6}$	0	$-\frac{1}{30}$	0	$\frac{1}{42}$	0
2	1	$\frac{1}{4}$	$-\frac{1}{36}$	$-\frac{1}{24}$	$\frac{7}{450}$	$\frac{1}{40}$	$-\frac{38}{2205}$	$-\frac{5}{168}$
3	1	$\frac{1}{8}$	$-\frac{11}{216}$	$-\frac{1}{288}$	$\frac{1243}{54000}$	$-\frac{49}{7200}$	$-\frac{75613}{3704400}$	$\frac{599}{35280}$
4	1	$\frac{1}{16}$	$-\frac{49}{1296}$	$\frac{41}{3456}$	$\frac{26291}{3240000}$	$-\frac{1921}{144000}$	$\frac{845233}{1555848000}$	$\frac{1048349}{59270400}$
5	1	$\frac{1}{32}$	$-\frac{179}{7776}$	$\frac{515}{41472}$	$-\frac{216383}{194400000}$	$-\frac{183781}{25920000}$	$\frac{4644828197}{653456160000}$	$\frac{153375307}{49787136000}$

定義および反復積分表示から次の 2 つの漸化式が導かれる．

命題 14.3 任意の $k\in\mathbf{Z}$ と $n\geq 0$ に対し

$$\mathbb{B}_n^{(k)}=\frac{1}{n+1}\left\{\mathbb{B}_n^{(k-1)}-\sum_{m=1}^{n-1}\binom{n}{m-1}\mathbb{B}_m^{(k)}\right\}.$$

ただし $n\leq 1$ のとき右辺の和は 0 とする．

証明 定義式に $1-e^{-t}$ をかけた $Li_k(1-e^{-t})=(1-e^{-t})\left(\sum_{n=0}^{\infty}\mathbb{B}_n^{(k)}\frac{t^n}{n!}\right)$ の両辺を t で微分する．$Li'_k(t)=\frac{1}{t}Li_{k-1}(t)$ より，

$$\frac{Li_{k-1}(1-e^{-t})}{1-e^{-t}}e^{-t}=e^{-t}\sum_{n=0}^{\infty}\mathbb{B}_n^{(k)}\frac{t^n}{n!}+(1-e^{-t})\sum_{n=1}^{\infty}\mathbb{B}_n^{(k)}\frac{t^{n-1}}{(n-1)!}.$$

両辺に e^t をかけて，$\dfrac{Li_{k-1}(1-e^{-t})}{1-e^{-t}}=\sum_{n=0}^{\infty}\mathbb{B}_n^{(k-1)}\dfrac{t^n}{n!}$ より，

$$\begin{aligned}\sum_{n=0}^{\infty}\mathbb{B}_n^{(k-1)}\frac{t^n}{n!}&=\sum_{n=0}^{\infty}\mathbb{B}_n^{(k)}\frac{t^n}{n!}+(e^t-1)\sum_{n=1}^{\infty}\mathbb{B}_n^{(k)}\frac{t^{n-1}}{(n-1)!}\\&=\sum_{n=0}^{\infty}\mathbb{B}_n^{(k)}\frac{t^n}{n!}+\sum_{l=1}^{\infty}\frac{t^l}{l!}\sum_{n=1}^{\infty}\mathbb{B}_n^{(k)}\frac{t^{n-1}}{(n-1)!}\\&=\sum_{n=0}^{\infty}\mathbb{B}_n^{(k)}\frac{t^n}{n!}+\sum_{n=1}^{\infty}\left(\sum_{m=0}^{n-1}\mathbb{B}_{m+1}^{(k)}\frac{1}{(n-m)!m!}\right)t^n\\&=\mathbb{B}_0^{(k)}+\sum_{n=1}^{\infty}\left(\mathbb{B}_n^{(k)}+\sum_{m=0}^{n-1}\binom{n}{m}\mathbb{B}_{m+1}^{(k)}\right)\frac{t^n}{n!}.\end{aligned}$$

よって，$n=0$ のとき $\mathbb{B}_0^{(k-1)}=\mathbb{B}_0^{(k)}$，$n\geq 1$ ならば

$$\mathbb{B}_n^{(k-1)}=\mathbb{B}_n^{(k)}+\sum_{m=0}^{n-1}\binom{n}{m}\mathbb{B}_{m+1}^{(k)}=(n+1)\mathbb{B}_n^{(k)}+\sum_{m=1}^{n-1}\binom{n}{m-1}\mathbb{B}_m^{(k)}.$$

あとは移項して $n+1$ で割ると命題が得られる． ∎

命題 14.4 $k\geq 1$ と $n\geq 0$ に対し

$$\mathbb{B}_n^{(k)}=\sum_{m=0}^{n}(-1)^m\binom{n}{m}\mathbb{B}_{n-m}^{(k-1)}\left(\sum_{l=0}^{m}\frac{(-1)^l}{n-l+1}\binom{m}{l}B_l\right).$$

証明 今度は反復積分表示を用いる．それによると

$$\frac{Li_k(1-e^{-t})}{1-e^{-t}}=\frac{e^t}{e^t-1}\int_0^t e^{-s}\frac{Li_{k-1}(1-e^{-s})}{1-e^{-s}}ds$$

であるので，

$$\begin{aligned}\sum_{n=0}^{\infty}\mathbb{B}_n^{(k)}\frac{t^n}{n!} &= \left(\sum_{n=0}^{\infty}B_n\frac{t^{n-1}}{n!}\right)\int_0^t\left(\sum_{n=0}^{\infty}\frac{(-s)^n}{n!}\right)\left(\sum_{n=0}^{\infty}\mathbb{B}_n^{(k-1)}\frac{s^n}{n!}\right)ds\\
&= \left(\sum_{n=0}^{\infty}B_n\frac{t^{n-1}}{n!}\right)\int_0^t\sum_{n=0}^{\infty}\left(\sum_{m=0}^{n}(-1)^{n-m}\binom{n}{m}\mathbb{B}_m^{(k-1)}\right)\frac{s^n}{n!}ds\\
&= \left(\sum_{n=0}^{\infty}B_n\frac{t^{n-1}}{n!}\right)\sum_{n=0}^{\infty}\left(\sum_{m=0}^{n}(-1)^{n-m}\binom{n}{m}\mathbb{B}_m^{(k-1)}\right)\frac{t^{n+1}}{(n+1)!}ds\\
&= \sum_{n=0}^{\infty}\left(\sum_{l=0}^{n}\frac{B_{n-l}}{l+1}\binom{n}{l}\left(\sum_{m=0}^{l}(-1)^{l-m}\binom{l}{m}\mathbb{B}_m^{(k-1)}\right)\right)\frac{t^n}{n!}\\
&= \sum_{n=0}^{\infty}\left(\sum_{m=0}^{n}(-1)^m\mathbb{B}_m^{(k-1)}\left(\sum_{l=m}^{n}\frac{(-1)^l}{l+1}\binom{n}{l}\binom{l}{m}B_{n-l}\right)\right)\frac{t^n}{n!}.\end{aligned}$$

ここで $\binom{n}{l}\binom{l}{m}=\binom{n}{m}\binom{n-m}{n-l}$ を使い，$l\to n-l$ とし，さらに $m\to n-m$ とすると，

$$\begin{aligned}&\sum_{m=0}^{n}(-1)^m\mathbb{B}_m^{(k-1)}\left(\sum_{l=m}^{n}\frac{(-1)^l}{l+1}\binom{n}{l}\binom{l}{m}B_{n-l}\right)\\
&\quad=\sum_{m=0}^{n}(-1)^m\binom{n}{m}\mathbb{B}_{n-m}^{(k-1)}\left(\sum_{l=0}^{m}\frac{(-1)^l}{n-l+1}\binom{m}{l}B_l\right)\end{aligned}$$

となり，命題がいえる．■

注意 14.5　2 つの漸化式はいずれも，$\mathbb{B}_n^{(k)}$ を表すのに $\mathbb{B}_n^{(k-1)}$ のように上つきインデックスの異なる数を必要としている．1 つの k の中での漸化式がつくれるかどうかはわかっていない．

ベルヌーイ数をスターリング数で書く公式（33 ページ定理 2.8）は多重ベルヌーイ数に対しても同じ形で一般化できる．

定理 14.6　$\mathbb{B}_n^{(k)}=(-1)^n\sum_{m=0}^{n}\frac{(-1)^m m!\left\{ {n \atop m} \right\}}{(m+1)^k}\qquad (n\geq 0,\ k\in\mathbf{Z}).$

証明　定理 2.8 の証明とまったく同様である．すなわち，28 ページ命題 2.6 (7) を使って，

$$\sum_{n=0}^{\infty} \mathbb{B}_n^{(k)} \frac{t^n}{n!} = \frac{Li_k(1-e^{-t})}{1-e^{-t}} = \sum_{m=1}^{\infty} \frac{(1-e^{-t})^{m-1}}{m^k}$$
$$= \sum_{m=0}^{\infty} \frac{(-1)^m (e^{-t}-1)^m}{(m+1)^k}$$
$$= \sum_{m=0}^{\infty} \frac{(-1)^m m!}{(m+1)^k} \sum_{n=m}^{\infty} \left\{ {n \atop m} \right\} \frac{(-t)^n}{n!}$$
$$= \sum_{n=0}^{\infty} (-1)^n \left(\sum_{m=0}^{n} \frac{(-1)^m m! \left\{ {n \atop m} \right\}}{(m+1)^k} \right) \frac{t^n}{n!}.$$

両辺の $\frac{t^n}{n!}$ の係数を比べれば求める公式が得られる. ∎

14.2 クラウゼン・フォンシュタウト型定理

この節では多重ベルヌーイ数の分母について論じる. 古典的なベルヌーイ数についてはクラウゼン・フォンシュタウトの定理（39 ページ定理 3.1）によって B_n の分母のみならず,「小数部分」が完全に決定されている. 一般の $\mathbb{B}_n^{(k)}$ についてはまだ以下の部分的な結果があるのみであるが, $k=2$ の場合（“di-Bernoulli” 数）については後で述べるように分母を完全に決定できる.

定理 14.7 k を 2 以上の自然数とし, p を $k+2 \le p \le n+1$ を満たす素数とする.

（1） $p-1 \mid n$ のとき, $p^k \mathbb{B}_n^{(k)} \in \mathbf{Z}_{(p)}$ （分母が p と素）で,

$$p^k \mathbb{B}_n^{(k)} \equiv -1 \mod p.$$

（2） $p-1 \nmid n$ のとき, $p^{k-1} \mathbb{B}_n^{(k)} \in \mathbf{Z}_{(p)}$ で,

$$p^{k-1}\mathbb{B}_n^{(k)} \equiv \begin{cases} \dfrac{1}{p}\left\{ {n \atop p-1} \right\} - \dfrac{n}{2^k} \mod p & n \equiv 1 \mod (p-1) \text{ のとき}, \\ \dfrac{(-1)^{n-1}}{p}\left\{ {n \atop p-1} \right\} \mod p & \text{その他}. \end{cases}$$

証明 有理数 a の p-order を $\mathrm{ord}_p(a)$ で表すとする. すなわち $\mathrm{ord}_p(p^t) = t$ で, $a \cdot p^{-\mathrm{ord}_p(a)}$ は分母分子ともに p と素である. 定理 3.1 の証明と同様に, 定理 14.6 の公式を用い, 各項の p-order を評価していく. $b_n^{(k)}(m) = \frac{(-1)^m m! \left\{ {n \atop m} \right\}}{(m+1)^k}$ とおき, (1) と (2) を同時に証明する.

$m+1=ap^e, (a,p)=1, e\geq 0$ と書く．もし $e=0$ ならば，$b_n^{(k)}(m)\in \mathbf{Z}_{(p)}$，そして $k\geq 2$ の仮定より $p^{k-1}b_n^{(k)}(m)\equiv 0 \mod p$ となるのでこの項は考えなくともよい．スターリング数 $\left\{ {n \atop m} \right\}$ は整数なので

$$\mathrm{ord}_p(b_n^{(k)}(m)) \geq \mathrm{ord}_p\left(\frac{m!}{(m+1)^k}\right)$$

となる．

まず $e\geq 2$ と仮定し，合同式 $p^k b_n^{(k)}(m)\equiv 0 \mod p$，さらに $p-1\nmid n$ のときは $p^{k-1}b_n^{(k)}(m)\equiv 0 \mod p$ が成り立つことを示す．$\mathrm{ord}_p(m!)=\sum_{j=1}^{\infty}\left[\frac{m}{p^j}\right]$ を使って以下のように評価をする．

$$\begin{aligned}\mathrm{ord}_p\left(\frac{m!}{(m+1)^k}\right) &= \sum_{j=1}^{\infty}\left[\frac{m}{p^j}\right]-ek \\ &\geq \left[\frac{m}{p}\right]-ek=\left[\frac{ap^e-1}{p}\right]-ek=ap^{e-1}-1-ek \\ &\geq p^{e-1}-1-ek=(1+p-1)^{e-1}-1-ek \\ &\geq 1+(e-1)(p-1)-1-ek=(e-1)(p-1)-ek \\ &\geq (e-1)(k+1)-ek=-k+e-1 \\ &\geq -k+1.\end{aligned}$$

これより $\mathrm{ord}_p\left(\frac{m!}{(m+1)^k}\right)\geq -k+1$ を得，したがって $p^{k-1}b_n^{(k)}(m)\in\mathbf{Z}_{(p)}$ となる．よって $p^k b_n^{(k)}(m)\equiv 0 \mod p$ である．もし上の不等号のうち 1 つでも真の不等号（$>$）が成り立てば，$p^{k-1}b_n^{(k)}(m)\equiv 0 \mod p$ を得る．すべての箇所で等号が成立するのは $e=2, m+1=p^2$ で $p=k+2$ のときであるが，このとき次の補題（$a=p$ の場合）により，$p-1\nmid n$ ならば $p^{k-1}b_n^{(k)}(m)\equiv 0 \mod p$ となる．

補題 14.8　n および a を自然数とする．このとき合同式

$$\left\{ {n \atop ap-1} \right\} \equiv \begin{cases} \dbinom{c-1}{a-1} \mod p & \exists c\geq a, n=a-1+c(p-1), \\ 0 \mod p & \text{その他} \end{cases}$$

が成り立つ．

証明　スターリング数 $\left\{{n \atop m}\right\}$ の母関数表示（28 ページ命題 2.6 (8)）

$$\sum_{n=m}^{\infty}\left\{{n \atop m}\right\}t^n = \frac{t^m}{(1-t)(1-2t)\cdots(1-mt)} \tag{14.2}$$

を用いる．$m = ap-1$ のときはこの式の右辺は p を法として

$$\begin{aligned}\frac{t^{ap-1}}{(1-t^{p-1})^a} &= t^{ap-1}\sum_{i=0}^{\infty}\binom{a+i-1}{i}t^{i(p-1)}\\ &= \sum_{i=0}^{\infty}\binom{a+i-1}{a-1}t^{a-1+(a+i)(p-1)}\end{aligned}$$

に等しい．（ここで $(1-t)(1-2t)\cdots(1-(p-1)t) \equiv 1-t^{p-1} \mod p$ を用いた．）$a+i=c$ とおけば補題が得られる．∎

次に $e=1$ $(m=ap-1)$ とする．もし $a \geq 3$ ならば $p^2|(ap-1)!$ であるので，$\mathrm{ord}_p\left(\frac{m!}{(m+1)^k}\right) > -k+1$ となり，これから $p^{k-1}b_n^{(k)}(m) \equiv 0 \mod p$ となる．$a=2$ のときは，$\mathrm{ord}_p(m!) = 1$ であって $\mathrm{ord}_p\left(\frac{m!}{(m+1)^k}\right) = 1-k$. よって $\mathrm{ord}_p(b_n^{(k)}(m)) = 1-k+\mathrm{ord}_p\left(\left\{{n \atop m}\right\}\right)$ となり，これから $p^k b_n^{(k)}(m) \equiv 0 \mod p$. $n \not\equiv 1 \mod (p-1)$ のときは上の補題で $a=2$ とすると $\left\{{n \atop 2p-1}\right\} \equiv 0 \mod p$ がわかる．これより $n \not\equiv 1 \mod (p-1)$ であれば $p^{k-1}b_n^{(k)}(m) \equiv 0 \mod p$. また $n \equiv 1 \mod (p-1)$ であれば $n = 1+c(p-1)$ と書くと，$c \geq 2$ であり（$n \geq m$ なので $c=1$ は起らない），再び補題より $\left\{{n \atop 2p-1}\right\} \equiv c-1 \equiv -n \mod p$ を得る．これから，

$$\begin{aligned}p^{k-1}b_n^{(k)}(m) &= p^{k-1}\frac{(-1)^{2p-1}(2p-1)!\left\{{n \atop 2p-1}\right\}}{(2p)^k}\\ &\equiv \frac{n}{2^k} \mod p\end{aligned}$$

となる．（ウィルソン[1]の定理 $(p-1)! \equiv -1 \mod p$ より $(2p-1)!/p \equiv ((p-1)!)^2 \equiv 1 \mod p$ を用いた．）

最後に，$a=1$ $(m=p-1)$ のときは，$b_n^{(k)}(m) = \frac{(p-1)!\left\{{n \atop p-1}\right\}}{p^k}$. 補題より $n \not\equiv 0 \mod (p-1)$ であれば $\left\{{n \atop p-1}\right\} \equiv 0 \mod p$ で，よって $p^{k-1}b_n^{(k)}(m) \equiv -\frac{1}{p}\left\{{n \atop p-1}\right\} \mod p$ となる．$n \equiv 0 \mod (p-1)$ であれば $\left\{{n \atop p-1}\right\} \equiv 1 \mod p$ か

[1] John Wilson（1741.8.6 イギリス Applethwaite 生——1793.10.18 イギリス Kendal 没）

つ $p^k b_n^{(k)}(m) \equiv -1 \mod p$.

以上を合わせ，定理が得られる． ∎

注意 14.9　k, p は定理のとおりとし，さらに $n \not\equiv 0, 1 \mod (p-1)$ とする．n' を，$n' \equiv n \mod p-1$ かつ $1 < n' < p$ を満たす唯一の整数とするとき，

$$p^{k-1}\mathbb{B}_n^{(k)} \equiv (n-n')\frac{B_n}{n} \mod p$$

が成り立つ．特に n が奇数のときは $p^{k-1}\mathbb{B}_n^{(k)} \equiv 0 \bmod p$ である．

これは，以下の定理 14.10 の証明中の (14.3) 式から

$$\frac{(-1)^{n-1}}{p}\left\{ {n \atop p-1} \right\} \equiv (n-n')\frac{B_n}{n} \mod p$$

がいえることによる．

2 重ベルヌーイ数の分母は次のように完全に記述できる．

定理 14.10

(1)　n が奇数のとき $\mathbb{B}_n^{(2)} = -\dfrac{(n-2)}{4}B_{n-1}$.（したがってこの場合分母の決定は本質的に古典的な場合に帰する.）

(2)　n を偶数 (≥ 2) とする．素数 p について $\mathbb{B}_n^{(2)}$ の p-order を $\mathrm{ord}(p,n)$ と書くとき，次が成り立つ．

(2-1)　$p > n+1$ ならば $\mathrm{ord}(p,n) \geq 0$.（分母に p が現れない.）

(2-2)　$5 \leq p \leq n+1$ なる p について，

(a)　$p-1 \mid n$ ならば $\mathrm{ord}(p,n) = -2$.

(b)　$p-1 \nmid n$ のとき

(b-1)　$p \mid \dfrac{B_n}{n}$ であるか，または $1 < n' < p-1$ なる n' があって $n \equiv n' \mod p(p-1)$ のとき $\mathrm{ord}(p,n) \geq 0$.

(b-2)　その他のとき $\mathrm{ord}(p,n) = -1$.

(2-3)　$n > 2$ かつ $n \equiv 2 \mod 3$ のとき $\mathrm{ord}(3,n) \geq 0$，その他のとき $\mathrm{ord}(3,n) = -2$.

(2-4)　$n > 2$ かつ $n \equiv 2 \mod 4$ のとき $\mathrm{ord}(2,n) \geq 0$，$n \equiv 0 \mod 4$ のとき $\mathrm{ord}(2,n) = -1, \mathrm{ord}(2,2) = -2$.

注意 14.11　(b-1) において現れる有理数 $\dfrac{B_n}{n}$ は常に $\mathbf{Z}_{(p)}$ の元である（Ireland-Rosen [43, Prop. 15.2.4] 参照）.

証明のために 1 つ補題を用意する．

補題 14.12 $n \geq 2$ を偶数，$p \geq 5$ を素数とし，$2p-1=m$ とする．このとき，

$$(-1)^m m! \left\{ {n \atop m} \right\} \equiv 0 \mod p^2.$$

したがって $\dfrac{(-1)^m m! \{ {n \atop m} \}}{(m+1)^2} \in \mathbf{Z}_{(p)}$.

証明 28 ページ命題 2.6 (6) より

$$(-1)^m m! \left\{ {n \atop m} \right\} = \sum_{l=1}^{2p-1} (-1)^l \binom{2p-1}{l} l^n$$

$$= \sum_{l=1}^{p-1} \left\{ (-1)^l \binom{2p-1}{l} l^n + (-1)^{2p-l} \binom{2p-1}{2p-l} (2p-l)^n \right\}$$

$$+(-1)^p \binom{2p-1}{p} p^n$$

$$\equiv \sum_{l=1}^{p-1} \left\{ (-1)^l \binom{2p-1}{l} l^n + (-1)^l \binom{2p-1}{l-1} (-2npl^{n-1} + l^n) \right\} \mod p^2.$$

ここで $\binom{2p-1}{l} + \binom{2p-1}{l-1} = \frac{2p}{l} \binom{2p-1}{l-1}$ であるので，最後の和は

$$2p(1-n) \sum_{l=1}^{p-1} (-1)^l \binom{2p-1}{l-1} l^{n-1}$$

に等しい．

$$\binom{2p-1}{l-1} \equiv (-1)^{l-1} \mod p$$

と，$p-1 \nmid n-1$ であること（n は偶数で p は奇数）より

$$\sum_{l=1}^{p-1} (-1)^l \binom{2p-1}{l-1} l^{n-1} \equiv -\sum_{l=1}^{p-1} l^{n-1} \equiv 0 \mod p.$$

■

定理 14.10 の証明 $\mathbb{B}_n^{(2)}$ の母関数の反復積分による表示 (14.1) と，$\frac{s}{e^s-1} = \sum_{l=0}^{\infty} (-1)^l B_l \frac{s^l}{l!}$ より

$$\sum_{n=0}^{\infty} \mathbb{B}_n^{(2)} \frac{t^n}{n!} = \frac{e^t}{e^t-1} \int_0^t \sum_{l=0}^{\infty} (-1)^l B_l \frac{s^l}{l!} ds$$

$$= \sum_{m=0}^{\infty} B_m \frac{t^{m-1}}{m!} \cdot \sum_{l=0}^{\infty} (-1)^l B_l \frac{t^{l+1}}{(l+1)!}.$$

これより

$$\mathbb{B}_n^{(2)} = \sum_{l=0}^{n}(-1)^l \binom{n}{l} \frac{B_{n-l}B_l}{l+1}$$

を得る．n が奇数のとき，$n-l, l$ の一方は奇数であって，奇数 $l \geq 3$ に対しては $B_l = 0$ であるので，$n \geq 3$ のとき

$$\mathbb{B}_n^{(2)} = -\frac{n}{2}B_{n-1}B_1 + B_1 B_{n-1} = -\frac{(n-2)}{4}B_{n-1}.$$

これは $n=1$ でも成り立つ．これで (1) が証明された．

(2-1) は定理 14.6 で与えた公式より自明．またその公式に現れる $\frac{m!}{(m+1)^2}$ が整数でないのは $m+1 = 8, 9$, 素数, $2\times$ 素数 のときのみであることが初等的に確かめられる．ところが補題 14.12 より，$m+1 = 2p$ (p は素数 ≥ 5) のとき $\frac{(-1)^m m! \left\{ n \atop m \right\}}{(m+1)^2}$ の分母に p が現れない．次に $\mathbb{B}_n^{(2)}$ の分母に寄与しうる項として $m+1=p$ (p は 5 以上の素数) のときを考えると，このとき

$$\begin{aligned}(-1)^m m! \left\{ n \atop m \right\} &= \sum_{l=1}^{p-1}(-1)^l \binom{p-1}{l} l^n \\ &\equiv \sum_{l=1}^{p-1} l^n \mod p.\end{aligned}$$

これは $\bmod p$ で，$p-1 \mid n$ なら -1 に，$p-1 \nmid n$ なら 0 に合同である．したがって $p-1 \mid n$ のとき $\frac{(-1)^m m! \left\{ n \atop m \right\}}{(m+1)^2}$ の p-order は -2．他の項は $\mathbf{Z}_{(p)}$ に入るから，これで (2-2)-(a) が示された．

$p-1 \nmid n$ とする．p^2 を法として

$$\binom{p-1}{l} \equiv (-1)^l + (-1)^{l-1} p \sum_{i=1}^{l} \frac{1}{i} \mod p^2$$

なること（$(p-1)(p-2)\cdots(p-l)$ を展開する）を用いると

$$\sum_{l=1}^{p-1}(-1)^l \binom{p-1}{l} l^n \equiv \sum_{l=1}^{p-1} l^n - p\sum_{l=1}^{p-1} l^n \sum_{i=1}^{l} \frac{1}{i} \mod p^2.$$

ところで n が偶数で $p-1 \nmid n$ のとき

$$\sum_{l=1}^{p-1} l^n \equiv pB_n \mod p^2$$

が知られている（Ireland-Rosen [43, Prop.15.2.2 の Cor.]）．一方 $n \equiv n' \mod p-1$, $1 < n' < p-1$ とすると，n' も偶数になり，Vandiver[2][85, (63)] より（注意 14.20 参照）

$$\sum_{l=1}^{p-1} l^n \sum_{i=1}^{l} \frac{1}{i} \equiv \sum_{l=1}^{p-1} l^{n'} \sum_{i=1}^{l} \frac{1}{i} \mod p$$
$$\equiv B_{n'} \mod p.$$

よって

$$(-1)^m m! \left\{ \begin{matrix} n \\ m \end{matrix} \right\} \equiv p\,(B_n - B_{n'}) \mod p^2.$$

$p-1 \nmid n$ であるので $\frac{B_n}{n} \in \mathbf{Z}_{(p)}$ かつ $B_{n'} \equiv n' \frac{B_n}{n} \mod p$ （[43, Prop.15.2.4, Th. 5]）．以上より（$m = p-1$）

$$(-1)^m m! \left\{ \begin{matrix} n \\ m \end{matrix} \right\} \equiv p(n - n') \frac{B_n}{n} \mod p^2 \tag{14.3}$$

となり，(2-2)-(b) がこれより従う．

3-order については，定理 14.6 の公式の和の項で，分母に 3 が現れ得るのは

$$\frac{2!\left\{ {n \atop 2} \right\}}{3^2}, \quad \frac{-5!\left\{ {n \atop 5} \right\}}{6^2}, \quad \frac{8!\left\{ {n \atop 8} \right\}}{9^2}$$

で，28 ページ命題 2.6 (6) を使ってそれぞれ計算することにより (2-3) が得られる．2-order についても同様に計算するが省略する． ∎

奇素数 p がベルヌーイ数 $B_2, B_4, \ldots, B_{p-3}$ の分子のいずれをも割り切らないとき，p を正則素数，いずれかを割り切るとき非正則素数という．Kummer によれば，p が非正則であることと，円の p 分体 $\mathbf{Q}(\zeta_p)$ の類数が p で割れることが同値である（Washington [88, §5.3] 参照）．

たとえば 100 以下の非正則素数は $37, 59, 67$ である．Kummer は（手計算で!）163 以下の素数について，正則，非正則を判定し，非正則な素数については，それぞれの p について何番目のベルヌーイ数の分子が p で割れるかを正しく与えている．それによれば引き続き $101, 103, 131, 149, 157$ が非正則素数で，$p = 157$ が $B_2, B_4, \cdots, B_{p-3}$ の 2 つの分子を割る最初の例となっている．（[88] の巻末

[2]Harry Schultz Vandiver（1882.10.21 アメリカ Philadelphia 生——1973.1.9 アメリカ Austin 没）

に 4001 までの非正則素数と，その素数で分子が割れるベルヌーイ数のインデックスの表がある.)

定理 14.2 の (2-2)-(b-1) に $p \mid \frac{B_n}{n}$ という条件がでてくることに注目すると，素数 p の非正則性を 2 重ベルヌーイ数 $\mathbb{B}_n^{(2)}$ の分母の言葉で述べることができる.

系 14.13　素数 $p\ (\geq 5)$ が非正則であるための必要十分条件は，範囲 $p+1 \leq n \leq 2p-4$ の中の偶数 n で，$\mathbb{B}_n^{(2)}$ の分母が p で割れないものが存在することである.

古典的なベルヌーイ数は，奇数番目は 0 で，偶数番目の分母は初等的に決めることができ（クラウゼン・フォンシュタウト），偶数番目の分子が円分体の整数論などと深く結びついた微妙な量である．この 2 重ベルヌーイ数は奇数番目が本質的に古典的ベルヌーイ数になり，偶数番目の分母の決定に古典的ベルヌーイ数の分子の情報を必要とする．さて，それでは 2 重ベルヌーイ数の分子と結びつくような面白い数論の対象はあるだろうか．それについてはいまのところわかっていない.

14.3　上指数が負の多重ベルヌーイ数

k が 0 または負のとき $\mathbb{B}_n^{(k)}$ は正の整数になり，前節で与えた公式とは別の，組み合わせ的に意味のつく公式で与えられることが示される．この節ではこれを紹介する．最初に表を与えておこう.

表 14.2: $\mathbb{B}_n^{(k)}$ $(-5 \leq k \leq 0,\ 0 \leq n \leq 7)$

k \ n	0	1	2	3	4	5	6	7
0	1	1	1	1	1	1	1	1
−1	1	2	4	8	16	32	64	128
−2	1	4	14	46	146	454	1394	4246
−3	1	8	46	230	1066	4718	20266	85310
−4	1	16	146	1066	6902	41506	237686	1315666
−5	1	32	454	4718	41506	329462	2441314	17234438

次が成り立つ．（この公式により $\mathbb{B}_n^{(-k)}$ に，場合の数としての意味をつける
ことができる．読者それぞれが考えてみられたい．）

定理 14.14 任意の $n, k \geq 0$ に対し，

$$\mathbb{B}_n^{(-k)} = \sum_{j=0}^{\min(n,k)} (j!)^2 \left\{ \begin{matrix} n+1 \\ j+1 \end{matrix} \right\} \left\{ \begin{matrix} k+1 \\ j+1 \end{matrix} \right\} \ (>0).$$

特に，

系 14.15（対称性） $\mathbb{B}_n^{(-k)} = \mathbb{B}_k^{(-n)}$.

証明[3] $\mathbb{B}_n^{(-k)}$ の 2 変数の母関数（指数関数型）を定理 14.6 と 28 ページ命題 2.6 (7) を用いて以下のように計算する．

$$\begin{aligned}
\sum_{n=0}^{\infty}\sum_{k=0}^{\infty} \mathbb{B}_n^{(-k)} \frac{x^n}{n!}\frac{y^k}{k!} &= \sum_{n=0}^{\infty}\sum_{k=0}^{\infty} (-1)^n \sum_{m=0}^{n} (-1)^m m! \left\{ \begin{matrix} n \\ m \end{matrix} \right\} (m+1)^k \frac{x^n}{n!}\frac{y^k}{k!} \\
&= \sum_{n=0}^{\infty} (-1)^n \sum_{m=0}^{n} (-1)^m m! \left\{ \begin{matrix} n \\ m \end{matrix} \right\} e^{(m+1)y} \frac{x^n}{n!} \\
&= \sum_{m=0}^{\infty} (-1)^m m! e^{(m+1)y} \sum_{n=m}^{\infty} (-1)^n \left\{ \begin{matrix} n \\ m \end{matrix} \right\} \frac{x^n}{n!} \\
&= \sum_{m=0}^{\infty} (-1)^m m! e^{(m+1)y} \frac{(e^{-x}-1)^m}{m!} \\
&= e^y \left(\frac{1}{1-(-e^y(e^{-x}-1))} \right) \\
&= \frac{e^{x+y}}{e^x+e^y-e^{x+y}}.
\end{aligned}$$

これをさらに

$$\begin{aligned}
\frac{e^{x+y}}{e^x+e^y-e^{x+y}} &= \frac{e^{x+y}}{1-(e^x-1)(e^y-1)} \\
&= e^{x+y} \sum_{j=0}^{\infty} (e^x-1)^j (e^y-1)^j \\
&= \sum_{j=0}^{\infty} \frac{1}{(j+1)^2} \frac{d}{dx}(e^x-1)^{j+1} \frac{d}{dy}(e^y-1)^{j+1}
\end{aligned}$$

とし，ここでまた命題 2.6 の (7) を使うと

[3] 以下の証明は落合啓之氏によるものである．もとの証明 [8] はかなり回りくどいものであった．簡単な別証をつけて下さった落合氏に感謝したい．

$$\sum_{n=0}^{\infty}\sum_{k=0}^{\infty}\mathbb{B}_n^{(-k)}\frac{x^n}{n!}\frac{y^k}{k!}=\sum_{j=0}^{\infty}(j!)^2\frac{d}{dx}\left(\sum_{n=j}^{\infty}\left\{{n+1 \atop j+1}\right\}\frac{x^{n+1}}{(n+1)!}\right)$$
$$\times\frac{d}{dy}\left(\sum_{k=j}^{\infty}\left\{{k+1 \atop j+1}\right\}\frac{y^{k+1}}{(k+1)!}\right)$$
$$=\sum_{j=0}^{\infty}\sum_{n=j}^{\infty}\sum_{k=j}^{\infty}(j!)^2\left\{{n+1 \atop j+1}\right\}\left\{{k+1 \atop j+1}\right\}\frac{x^n}{n!}\frac{y^k}{k!}$$

となる．両辺の係数を比較して定理を得る（$j>\min(n,k)$ のとき $\left\{{n+1 \atop j+1}\right\}\left\{{k+1 \atop j+1}\right\}=0$ に注意）．∎

定理より，証明中に得たものとは違う型の母関数表示が得られる．

系 14.16

$$\sum_{n=0}^{\infty}\sum_{k=0}^{\infty}\mathbb{B}_n^{(-k)}x^ny^k=\sum_{j=0}^{\infty}p_j(x)p_j(y),$$

ここに

$$p_j(x)=\frac{j!x^j}{(1-x)(1-2x)\cdots(1-(j+1)x)}.$$

証明　命題 2.6 (8) より

$$p_j(x)=j!\sum_{n=j}^{\infty}\left\{{n+1 \atop j+1}\right\}x^n$$

であるから，定理より直ちに従う．∎

この母関数を違った形に計算して，次の等式を示すことができる．

命題 14.17　任意の $n>0$ に対し

$$\sum_{l=0}^{n}(-1)^l\mathbb{B}_{n-l}^{(-l)}=0.$$

この式は，系 14.15 の対称性から n が奇数のときは自明な式になるが，n が偶数のときは非自明なことを述べている．たとえば 表 14.2 より $1-2+1=0$, $1-8+14-8+1=0$, など．

証明　系 14.16 の左辺を $B(x,y)$ とおく．定理 14.6 と 28 ページ命題 2.6 (8) を用いて変形すると，

$$B(x,y)=\sum_{n=0}^{\infty}\sum_{k=0}^{\infty}(-1)^n\sum_{m=0}^{n}(-1)^m m!\left\{ {n \atop m} \right\}(m+1)^k x^n y^k$$
$$=\sum_{m=0}^{\infty}(-1)^m m!\sum_{n=m}^{\infty}(-1)^n\left\{ {n \atop m} \right\}x^n\frac{1}{1-(m+1)y}$$
$$=\sum_{m=0}^{\infty}\frac{m!x^m}{(1+x)(1+2x)\cdots(1+mx)(1-(m+1)y)}.$$

($m=0$ の項は $\frac{1}{1-y}$.) ここで $y=-x$ とし，命題 2.6 (8) と $m!=\left[{m+1 \atop 1} \right]$，および命題 2.6 (5.1) を使うと $B(x,-x)=1$ が示される．これより命題がでる．■

最後に，定理 14.6 の公式と系 14.15 の対称性を応用して，Vandiver によるある定理（の特別な場合）を証明しよう．

定理 14.18 奇素数 p と $1\le i\le p-2$ なる i について

$$B_i\equiv\sum_{m=1}^{p-2}\left(1+\frac{1}{2}+\cdots+\frac{1}{m}\right)(m+1)^i \mod p.$$

証明 $B_i=\mathbb{B}_i^{(1)}$ である．定理 14.6 とフェルマーの小定理より

$$\mathbb{B}_i^{(1)}\equiv\mathbb{B}_i^{(2-p)} \mod p$$

が成り立つ．この右辺は系 14.15 より $\mathbb{B}_{p-2}^{(-i)}$ に等しく，これに再び定理 14.6 を用いて

$$B_i\equiv-\sum_{m=0}^{p-2}(-1)^m m!\left\{ {p-2 \atop m} \right\}(m+1)^i.$$

したがって次の補題がいえればよい（$\left\{ {p-2 \atop 0} \right\}=0$）．

補題 14.19 $1\le m\le p-2$ とするとき

$$(-1)^{m-1}m!\left\{ {p-2 \atop m} \right\}\equiv 1+\frac{1}{2}+\cdots+\frac{1}{m} \mod p.$$

証明 $(-1)^{m-1}m!\left\{ {p-2 \atop m} \right\}=b_m$ と書くと，スターリング数の漸化式 (2.1)（24 ページ）より，

$$(-1)^{m-1}m!\left\{ {p-1 \atop m} \right\}=m(-b_{m-1}+b_m) \qquad (m\ge 2).$$

一方 28 ページ命題 2.6 (6) より

$$
\begin{aligned}
(-1)^{m-1}m!\left\{{p-1 \atop m}\right\} &= -\sum_{l=1}^{m}(-1)^l\binom{m}{l}l^{p-1} \\
&\equiv -\sum_{l=1}^{m}(-1)^l\binom{m}{l} \mod p \\
&\equiv 1 \mod p.
\end{aligned}
$$

よって $b_m \equiv b_{m-1} + \frac{1}{m} \mod p$.

これと，$b_1 = \left\{{p-2 \atop 1}\right\} = 1$ より補題がいえて，定理が証明された． ∎

注意 14.20　$1 < i \le p-2$ に対しては，定理の右辺は

$$
\sum_{m=1}^{p-1}\left(1 + \frac{1}{2} + \cdots + \frac{1}{m}\right)m^i
$$

と合同になることがわかる．この式と B_i が p を法として合同である，というのがもとの合同式 [85, (63)] の特別な場合である（Vandiver はベルヌーイ数として $B_1 = -\frac{1}{2}$ のほうを採用しているので $i = 1$ でも成り立つ）．

参考文献

[1] S. Akiyama and Y. Tanigawa : Multiple zeta values at non-positive integers, preprint (1999).

[2] A. N. Andrianov : *Quadratic Forms and Hecke Operators*, Grundlehren der mathematischen Wissenshaften, **286**, Springer-Verlag, 1987.

[3] R. Apéry : Irrationalité de $\zeta(2)$ et $\zeta(3)$, *Astérisque*, **61** (1979), 11–13.

[4] T. Arakawa : Generalized eta-functions and certain ray class invariants of real quadratic fields, *Math. Ann.*, **260** (1982), 475–494.

[5] T. Arakawa : Dirichlet series $\sum_{n=1}^{\infty}(\cot \pi n\alpha)/n^s$, Dedekind sums, and Hecke L-functions for real quadratic fields, *Comment. Math. Univ. St. Pauli*, **37** (1988), 209–235.

[6] T. Arakawa : A note on the Hirzebruch sum, *Comment. Math. Univ. St. Pauli*, **42** (1993), 81–92.

[7] T. Arakawa and M. Kaneko : Multiple zeta values, poly-Bernoulli numbers, and related zeta functions, *Nagoya Math. J.*, **153** (1999), 189–209.

[8] T. Arakawa and M. Kaneko : On poly-Bernoulli numbers, *Comment. Math. Univ. St. Pauli*, **48** (1999), 159–167.

[9] E. Barnes : The genesis of the double gamma functions, *Proc. London Math. Soc.*, **31** (1899), 358–381.

[10] E. Barnes : The theory of the double gamma functions, *Philos. Trans. Roy. Soc.* (A), **196** (1901), 265–388.

[11] L. Berggren, J. Borwein and P. Borwein : *Pi : A Source Book*, Springer-Verlag, New York, 1997.

[12] B. C. Berndt : Dedekind sums and a paper of G. H. Hardy, *J. London Math. Soc.*, **13** (1976), 129–137.

[13] B. C. Berndt, R. J. Evans, and K. S. Williams : *Gauss and Jacobi Sums*, Canadian Math. Soc. series of monographs and avdanced texts, Vol. 21, A Wiley-Interscience Publication, 1998.

[14] C. A. ビエルクネス :『わが数学者アーベル—その生涯と発見—』, 辻雄一訳, 現代数学社, 1991.

[15] K.-R. Biermann : Thomas Clausen, Mathematiker und Astronom, *J. Reine Angew. Math.*, **216** (1964), 159–198.

[16] K.-R. Biermann : Kummer, Ernst Eduard, in ***Dictionary of Scientific Biography***, Vol. 7 & 8, Charles Scribner's Sons, New York, 1981.

[17] T. Clausen : Ueber die Fälle, wenn die Reihe von der Form $y = 1 + \frac{\alpha}{1} \cdot \frac{\beta}{\gamma} x + \frac{\alpha . \alpha+1}{1.2} \cdot \frac{\beta . \beta+1}{\gamma . \gamma+1} x^2 +$ etc. ein Quadrat von der Form $z = 1 + \frac{\alpha'}{1} \cdot \frac{\beta'}{\gamma'} \frac{\delta'}{\varepsilon'} x + \frac{\alpha' . \alpha'+1}{1.2} \cdot \frac{\beta' . \beta'+1}{\gamma' . \gamma'+1} \cdot \frac{\delta' . \delta'+1}{\varepsilon' . \varepsilon'+1} x^2 +$ etc. hat, *J. Reine Angew. Math.*, **3** (1828), 89–91.

[18] T. Clausen : Über die Function $\sin\varphi + \frac{1}{2^2}\sin 2\varphi + \frac{1}{3^2}\sin 3\varphi +$ etc., *J. Reine Angew. Math.*, **8** (1832), 298–300.

[19] T. Clausen : Beweis, daß die algebraischen Gleichungen Wurzeln von der Form $a + bi$ haben, *Astron. Nachr.*, **17** (1840), 325–330.

[20] T. Clausen : Lehrsatz aus einer Abhandlung über die Bernoullischen Zahlen, *Astron. Nachr.*, **17** (1840), 351–352.

[21] J. Coates and A. Wiles : Kummer's criterion for Hurwitz numbers, in Algebraic number theory (Kyoto Internat. Sympos., RIMS, Kyoto, 1976), Japan Soc. Promotion Sci., Tokyo (1977), 9–23.

[22] P. G. L. Dirichlet : ***Lectures on Number Theory***, with Supplements by R. Dedekind, History of Mathematics Sources, Vol. 16, Amer. Math. Soc., 1999.

[23] A. W. F. Edwards : A quick route to sums of powers, *Amer. Math. Monthly*, **93** (1986), 451–455.

[24] L. Euler : Remarques sur un beau rapport entre les séries des puissances tant directes que réciproques (1749), Opera omnia（全集), series prima XV, 70–90.

[25] L. Euler : De numero memorabili in summatione progressionis harmonicae naturalis occurrente (1785), Opera omnia（全集), series prima XV, 567–603.

[26] H. Freudenthal : Hurwitz, Adolf, in ***Dictionary of Scientific Biography***, Vol. 5 & 6, Charles Scribner's Sons, New York, 1981.

[27] C. Gauss :『ガウス整数論』, 高瀬正仁訳, 朝倉書店, 1995.（原著: ***Disquisitiones Arithmeticae***, 1801.）

[28] H. G. Gould : Explicit formulas for Bernoulli numbers, *Amer. Math. Monthly*, **79** (1972), 44–51.

[29] R. Graham, D. Knuth, and O. Patashnik :『コンピュータの数学』, 有澤誠・安村通晃・萩野達也・石畑清訳, 共立出版, 1993.（原著: ***Concrete Mathematics***, Addison-Wesley, 1989.）

[30] K. Hashimoto : Representation of the finite symplectic group $Sp(2, \mathbf{F}_p)$ in the space of Siegel modular forms, *Contemporary Math.*, **53** (1986), 253–276.

[31] K. Hensel : ***Festschrift zur Feier des 100. Geburtstages Eduard Kummers***, B. G. Teubner, 1910 (Kummer 全集 33–69).

[32] D. Hilbert : Adolf Hurwitz, Gedächtnisrede, ***Nachrichten von der k. Gesellshaft der Wissenschaften zu Göttingen*** (1920), 75–83 (Hurwitz 全集 I xiii–xx).

[33] 平松豊一：『数論を学ぶ人のための相互法則入門』, 数理情報科学シリーズ 18, 牧野書店, 1998.

[34] 平山諦：『東西数学物語』, 恒星社厚生閣, 1956.

[35] 平山諦：『関孝和—その業績と伝記—』, 恒星社厚生閣, 1959.

[36] A. Hurwitz : Einige Eigenschaften der Dirichlet'schen Funktionen $F(s) = \sum \left(\frac{D}{n}\right) \cdot \frac{1}{n^s}$, die bei der Bestimmung der Klassenanzahlen binärer quadratischer Formen auftreten, *Zeitschrift für Math. und Physik*, **27** (1882), 86–101 (全集 I 72–88).

[37] A. Hurwitz : Über die Entwicklungskoeffizienten der lemniskatischen Funktionen, *Math. Ann.*, **51** (1899), 196–226 (全集 I 342–373).

[38] T. Ibukiyama : On some elementary character sums, *Comment. Math. Univ. St. Pauli*, **47** (1998), 7–13.

[39] T. Ibukiyama and H. Saito : On zeta functions associated to symmetric matrices and an explicit conjecture on dimensions of Siegel modular forms of general degree, *International Mathematical Research Notices*, **8** (1992), 161–169.

[40] T. Ibukiyama and H. Saito : On a L-functions of ternary zero forms and exponential sums of Lee and Weintraub, *J. Number Theory*, **48-2** (1994), 252–257.

[41] T. Ibukiyama and H. Saito : On zeta functions associated to symmetric matrices I: *Amer. J. Math.*, **117-5** (1995), 1097–1155; II: preprint; III: *Nagoya Math. J.*, **146** (1997), 149–183.

[42] 伊吹山知義・齋藤裕：「やさしい」ゼータ関数について, 日本数学会『数学』, 50 巻 1 号 (1998), 1–11.

[43] K. Ireland and M. Rosen : *A Classical Introduction to Modern Number Theory*, Second Edition, Graduate Texts in Mathematics **84**, Springer-Verlag, 1990.

[44] 伊藤清三：『ルベーグ積分』, 数学選書 4 , 裳華房, 1963.

[45] K. Iwasawa : Lectures on p-adic L-functions, *Ann. of Math. Studies*, **74**, Princeton Univ. Press, Princeton, N.J., 1972.

[46] C. G. J. Jacobi : De usu legitimo formulae summatoriae Maclaurinianae, *J. Reine Angew. Math.*, **12** (1834), 263–272 (全集 VI 64–75).

[47] Ch. Jordan : *Calculus of Finite Differences*, Chelsea Publ. Co., New York, 1965. （初版 Budapest, 1939.）

[48] M. Kaneko : A generalization of the Chowla-Selberg formula and the zeta functions of quadratic orders, *Proc. Japan Acad.*, **66(A)-7** (1990), 201–203.

[49] M. Kaneko : A recurrence formula for the Bernoulli numbers, *Proc. Japan Acad.*, **71(A)-8** (1995), 192–193.

[50] M. Kaneko : Poly-Bernoulli numbers, *Jour. Th. Nombre Bordeaux*, **9** (1997), 199–206.

[51] N. Katz : The congruences of Clausen-von Staudt and Kummer for Bernoulli-Hurwitz numbers, *Math. Ann.*, **216** (1975), 1–4.

[52] D. Knuth : Two notes on notation, *Amer. Math. Monthly*, **99** (1992), 403–422.

[53] D. Knuth : Johann Faulhaber and sum of powers, *Math. Comp.*, **61** no. 203 (1993), 277–294.

[54] D. Knuth and T. J. Buckholtz : Computation of tangent Euler and Bernoulli numbers, *Math. Comp.*, **21** (1967), 663–688.

[55] L. Kronecker : Bemerkungen zur Abhandlung des Herrn Worpitzky, *J. Reine Angew. Math.*, **94** (1883), 268–270 (全集 II 405–407).

[56] E. E. Kummer : Über die hypergeometrische Reihe $1+\frac{\alpha\cdot\beta}{1\cdot\gamma}x+\frac{\alpha(\alpha+1)\beta(\beta+1)}{1\cdot 2\cdot\gamma(\gamma+1)}x^2+\frac{\alpha(\alpha+1)(\alpha+2)\beta(\beta+1)(\beta+2)}{1\cdot 2\cdot 3\cdot\gamma(\gamma+1)(\gamma+2)}x^3+\ldots$, *J. Reine Angew. Math.*, **15** (1836), 39–83, 127–172 (全集 II 75–166). この論文の長岡半太郎による英訳が, 東京数学物理学会記事巻の四 (1891), 276–325, 353–405 にある.

[57] E. E. Kummer : Über eine allgemeine Eigenschaft der rationalen Entwicklungscoefficienten einer bestimmten Gattung analytischer Functionen, *J. Reine Angew. Math.*, **41** (1851), 368–372 (全集 I 358–362).

[58] E. Lampe : Nachruf für Ernst Eduard Kummer, *Jahresbericht der Deutschen Mathematiker-vereinigung*, **3** (1894), 13–21 (Kummer 全集 I 15–30).

[59] S. Lang : *Cyclotomic Fields*, Graduate Texts in Mathematics **59**, Springer-Verlag, 1980.

[60] S. Lang : *Elliptic Functions*, Second Edition, Graduate Text in Mathematics **112**, Springer-Verlag, 1987. 旧版は Addison-Wesley Publishing Company Inc., 1973.

[61] R. Lee and S. H. Weintraub : On a generalization of a theorem of Erich Hecke, *Proc. Nat. Acad. Sci. U.S.A.*, **79** (1982), 7955–7957.

[62] F. Lindemann : Ueber die Zahl π, *Math. Ann.*, **20** (1882), 213–225.

[63] E. Meissner : Gedächtnisrede auf Adolf Hurwitz, *Vierteljahrsschrift der Naturforschenden Gesellschaft in Zürich*, **64** (1919), 855–857.

[64] 森本光生 :『UBASIC による解析入門』, 日本評論社, 1992.

[65] N. Nielsen : *Handbuch der Theorie der Gammafunktion*, Chelsea Publ. Co., New York, 1965. (初版 Leipzig, 1906.)

[66] 日本学士院編 :『明治前 日本数学史』, 岩波書店, 1956.

[67] M. Noether : Zur Erinnerung an Karl Georg Christian von Staudt, *Jahresbericht d. Deutschen Mathem.-Vereinigung*, **32** (1923), 97–119.

[68] N. E. Nörlund : *Vorlesungen über Differenzenrechnung*, Chelsea Publ. Co., New York, 1954. (初版 Springer-Verlag, Berlin, 1924.)

[69] G. Pólya : Some mathematicians I have known, *Amer. Math. Monthly*, **76** (1969), 746–753.

[70] C. リード：『ヒルベルト—現代数学の巨峰—』, 彌永健一訳, 岩波書店, 1972.

[71] H. F. Scherk : Über einen allgemeinen, die Bernoullischen Zahlen und die Coëfficienten der Secantenreihe zugleich darstellenden Ausdruck, *J. Reine Angew. Math.*, **4** (1829), 299–304.

[72] J.-P. Serre : *Formes modulaires et fonctions zêta p-adiques*, Lect. Notes in Math., no. 350, Springer-Verlag (1973), 191–268 (全集 III 95–172).

[73] J.-P. Serre : 『数論講義』, 彌永健一訳, 岩波書店, 1979. （原著: *Cours d'arithmétique*, Presses Universitaires de France, 1970, 英訳 *A course in Arithmetic*, Graduate Text in Mathematics **7**, Springer-Verlag, 1973.）

[74] 関孝和：『関孝和全集』, 平山諦・下平和夫・広瀬秀雄編著, 大阪教育図書, 1974.

[75] T. Shintani : On a Kronecker limit formula for real quadratic fields, *J. Fac. Sci. Univ. Tokyo, Sec.IA*, **24** (1977), 167–199.

[76] T. Shintani : 代数体の L-関数の特殊値について, 日本数学会『数学』, 29 巻 3 号 (1977), 204–216.

[77] T. Shintani: On certain ray class invariants of real quadratic fields, *J. Math. Soc. Japan*, **30** (1978), 139–167.

[78] I. Sh. Slavutskii : Staudt and arithmetical properties of Bernoulli numbers, *Historia Scientiarum*, **5-1** (1995), 69–74.

[79] 鈴木通夫：『群論（上）』, 岩波書店, 1977.

[80] 高木貞治：『初等整数論講義第 2 版』, 共立出版, 1971.

[81] 高橋礼司：『複素解析』, 東京大学出版会, 1990.

[82] R. Tsushima : The spaces of Siegel cusp forms of degree two and the representation of $Sp(2, \mathbf{F}_p)$, *Proc. Japan Acad.*, **60** (1984), 209–211.

[83] R. Tsushima : Dimension formula for the spaces of Siegel cusp forms and a certain exponential sum, *Mem. Inst. Sci. Tech. Meiji University*, **36** (1997), 1–56.

[84] 梅村浩：『楕円関数論』, 東京大学出版会, 2000.

[85] H. S. Vandiver : On developments in an arithmetic theory of the Bernoulli and allied numbers, *Scripta Math.*, **25** (1961), 273–303.

[86] K. G. C. von Staudt : Beweis eines Lehrsatzes, die Bernoullischen Zahlen betreffend, *J. Reine Angew. Math.*, **21** (1840), 372–374.

[87] K. G. C. von Staudt : Beweis des Satzes, daß jede algebraische rationale ganze Function von einer Veränderlichen in Faktoren vom ersten Grade aufgelöst werden kann, *J. Reine Angew. Math.*, **29** (1845), 97–102.

[88] L. C. Washington : *Introduction to Cyclotomic Fields*, Graduate Text in Mathematics **83**, Springer-Verlag, 1982.

[89] H. Weber : *Lehrbuch der Algebra Vol. III*, Chelsea Publ. Co., New York. （初版 Friedrich Vieweg und Sohn, Braunschweig, 1908.）

[90] A. Weil :『数論 歴史からのアプローチ』, 足立恒雄・三宅克哉訳, 日本評論社, 1987. (原著: *Number Theory: An Approach Through History; From Hammurapi to Legendre*, Birkhäuser Boston, 1983.)

[91] E. T. Whittaker and G. N. Watson : *A Course of Modern Analysis*, Cambridge University Press, 1927.

[92] D. Zagier : A Kronecker limit formula for real quadratic fields, *Math. Ann.*, **213** (1975), 153–184.

[93] D. Zagier : Modular forms whose Fourier coefficients involve zeta functions of quadratic fields, in *Modular functions of one variable VI*, Lect. Notes in Math., no. 627, Springer-Verlag (1977), 105–169.

[94] D. Zagier :『数論入門 (ゼータ関数と 2 次体)』, 片山孝次訳, 岩波書店, 1990. (原著: *Zetafunktionen und quadratische Körper*, Springer-Verlag, 1981.)

[95] D. Zagier : A one-sentence proof that every prime $p \equiv 1 \pmod 4$ is a sum of two squares, *Amer. Math. Monthly*, **97-2** (1990), 144.

[96] D. Zagier, : Values of zeta functions and their applications, in ECM volume, *Progress in Math.*, **120** (1994), 497-512.

人名索引

事項索引

さ　行

ま　行

や　行

ら　行

わ　行

著者紹介

荒川恒男 (あらかわ　つねお)

1975 年東京大学大学院理学系研究科数学専攻修士課程終了．現在立教大学理学部教授，理学博士．

伊吹山知義 (いぶきやま　ともよし)

1973 年東京大学大学院理学系研究科数学専攻修士課程終了．東京大学助手，九州大学助教授，大阪大学教授を経て，現在大阪大学大学院理学研究科教授，理学博士．

金子昌信 (かねこ　まさのぶ)

1988 年東京大学大学院理学系研究科数学専攻博士課程終了．大阪大学助手，京都工芸繊維大学助教授を経て，現在九州大学大学院数理学研究院助教授，理学博士．

ベルヌーイ数とゼータ関数

2001 年 7 月 1 日　初版第 1 刷発行

著　者--------荒川恒男
伊吹山知義
金子昌信

発行者--------牧野末喜

発行所--------(有)牧野書店

〒114-0024 東京都北区西ヶ原 3-60-18
電話(03)3949-2344・振替 00190-0-661932

発売所--------(株)星雲社

〒112-0012 東京都文京区大塚 3-21-10
電話(03)3947-1021・FAX(03)3947-1617

印刷・製本----大日本法令印刷(株)

ISBN4-7952-0139-0 C3041